Micro Focus Security
ArcSight ESM CIP for FISMA

Software Version: 6.0

Solutions Guide

Document Release Date: June, 2018
Software Release Date: June, 2018

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Overview & Architecture

This chapter contains an overview of the Compliance Insight Package for FISMA (CIP for FISMA) and contains the following topics:

The Federal Information Security Management Act (FISMA) of 2002 stipulates that all United States federal agencies must follow a set of processes in order to protect their information systems. The National Institute of Standards and Technology (NIST) is responsible for developing and publishing a set of standards and guidelines for securing information systems such as Federal Information Processing Standards or FIPS.

NIST 800-53

The NIST Special Publication 800-53 defines the selection and employment of appropriate security controls for an information system. NIST 800-53 defines security controls as management, operational, and technical safeguards, or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. In addition, NIST 800-53 defines 20 security control families as defined by the following table. Each security control family contains a set of related security controls. For example, the Access Control family contains 25 security controls. Each security control has a unique identifier that contains two characters representing the security control, a hyphen (-) followed by a number. For example, the first security control in the Access Control family is called Access Control Policy and Procedure, and is referenced using the AC-1 identifier. CIP for ESM Use cases, lists the security controls and the CIP for FISMA use cases that help address each control.

The following table defines the 20 security control families defined by the NIST.

Table 1-1 NIST Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

NIST 800-63

The NIST Special Publication 800-63 is the Electronic Authentication Guideline. NIST provides the following abstract to describe the NIST 800-63 guidance:

This recommendation provides technical guidance to Federal agencies implementing electronic authentication, and coverage for users' remote authentication over open networks. It defines technical requirements for each four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

You can download a PDF of the NIST 800-63 document from the following URL:
http://csrc.nist.gov/publications/PubsSPs.html

The authentication levels provided in NIST 800-63 are used by the following use case: E-Authentication Overview.

CIP for FISMA

Compliance Insight Package for FISMA (CIP for FISMA) provides an essential foundation for your FISMA compliance program. CIP for FISMA uses ArcSight™ ESM features, such as event categorization, threat prioritization, trends, workflow, and case management, to easily identify and address activities and anomalies involving systems that are subject to FISMA compliance. CIP for FISMA is made up of a comprehensive and easily customizable set of ArcSight ESM resources (rules, dashboards, data monitors, reports, and so on), which enable you to measure and report your compliance with FIPS using best practices outlined by NIST 800-53 and NIST 800-63 standards in relation to the following objectives:

- Compliance reporting—Supports the presentation of requirements to internal and external audit teams, as well as upper management.
- Real-time detection of compliance breaches—Pro-actively addresses compliance violations.
- Security best practices—Due diligence in complying with NIST 800-53 standard, as well as security policies and best practices.
- Automation of Monitoring-IT control—CIP for FISMA follows and adapts to changes in the IT environment. More than 200 correlation rules can be used to monitor policy compliance violations in real-time.
- Harmful User and Machine Monitoring – Tracks potentially harmful users and machines.
- Visualizing Security Events – Displaying security events graphically allows for a quick analysis of each situation.
- Vulnerabilities and Configuration changes Monitoring – Tracking vulnerabilities and configuration changes.

NIST Publications

NIST has developed the following documents to define standards and guidelines to provide information security for organization operations and assets:

- NIST Special Publication 800-53—Recommended Security Controls for Federal Information System.
- NIST Special Publications 800-63—Electronic Authentication Guideline.
- FIPS-199—Standards for Security Categorization of Federal Information and Information Systems.

FIPS 199

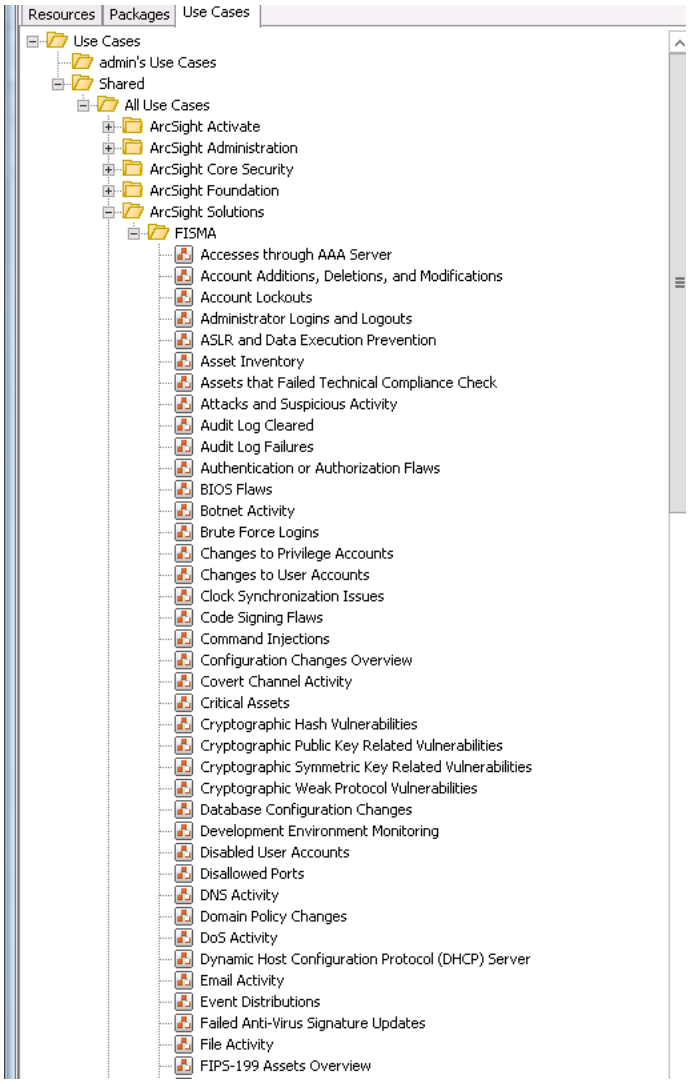
The FIPS PUB 199 document provides Standards for Security Categorization of Federal Information and Information Systems. NIST created FIPS Publication 199 to develop standards for categorizing information and information systems. You can download a PDF of the FIPS PUB 199 document from the following URL: http://csrc.nist.gov/publications/fips

The categorizations provided in FIPS-199 are used by the following use cases:

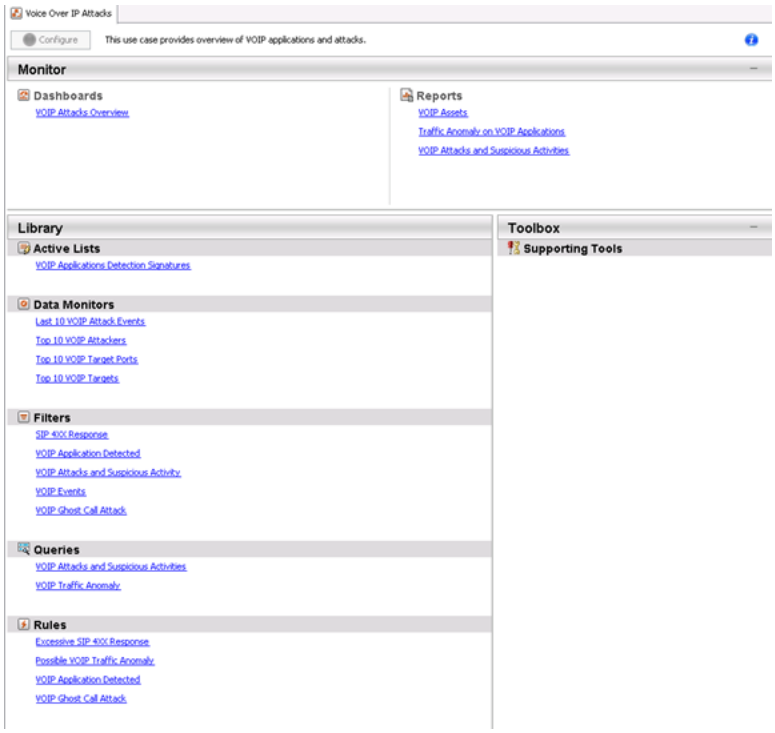
- New Systems
- NIST 800-53 Impact Assets Overview
- FIPS-199 Assets Overview

Solution Architecture

CIP for FISMA helps to ensure compliance with FISMA requirements by providing a set of use cases that address and support the NIST 800-53 security controls. Resources are organized into use cases by security purpose or area such as Audit Log Cleared or Password Management. These use cases are represented in ArcSight ESM as use case resources and provide a central location for managing content. The CIP for FISMA use cases are listed in the Use Case tab of the Navigator panel as shown in the following figure:

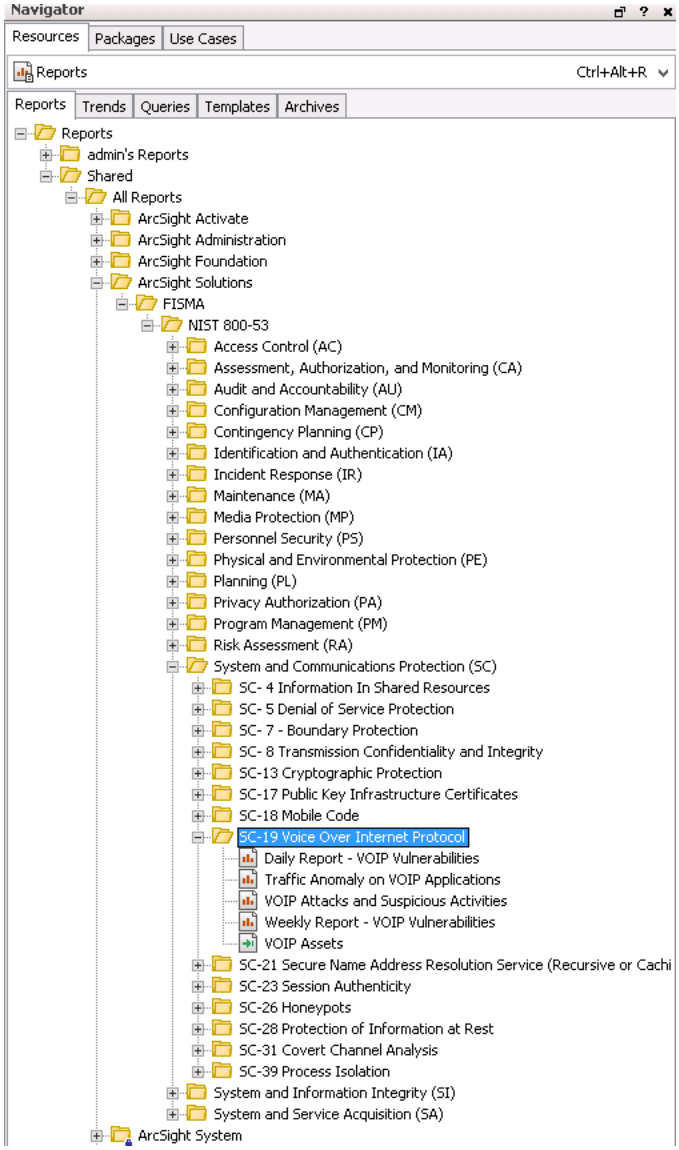


For example, the following figure shows the resources that make up the Voice Over IP Attacks use case resource.



Resources are also organized by NIST Security Controls, for example all the resources which help with specific NIST 800-53 control are stored in the corresponding group on the resource navigator.

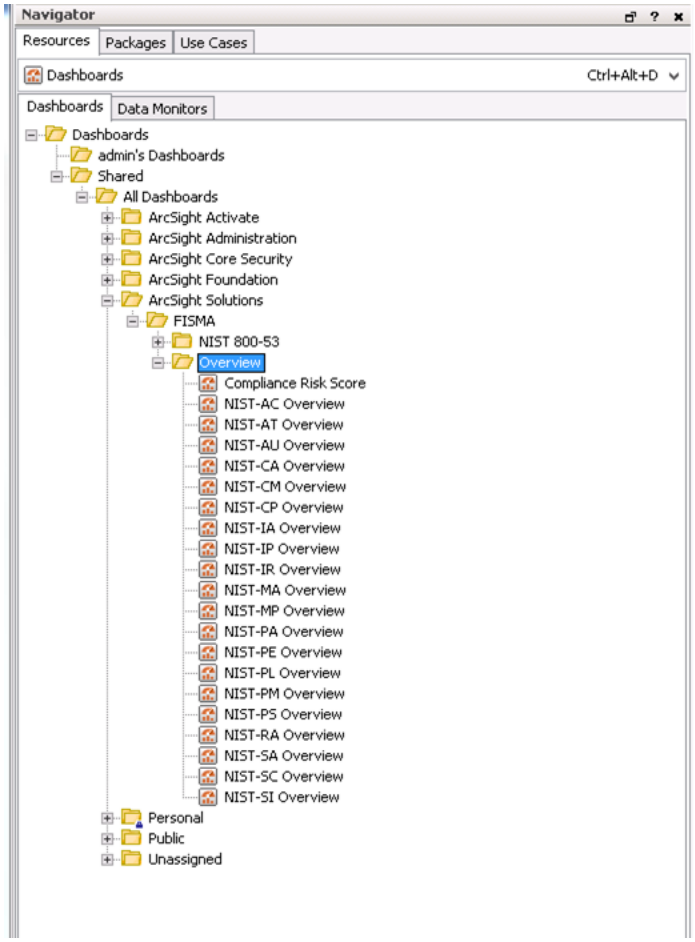
For example all the reports which help with control SC-19 are stored under SC-19 group as shown in the following figure:



In addition to the resources supplied to help address specific NIST 800-53 control, there are a common set of filters and active lists that support the entire solution.

Overview Dashboards

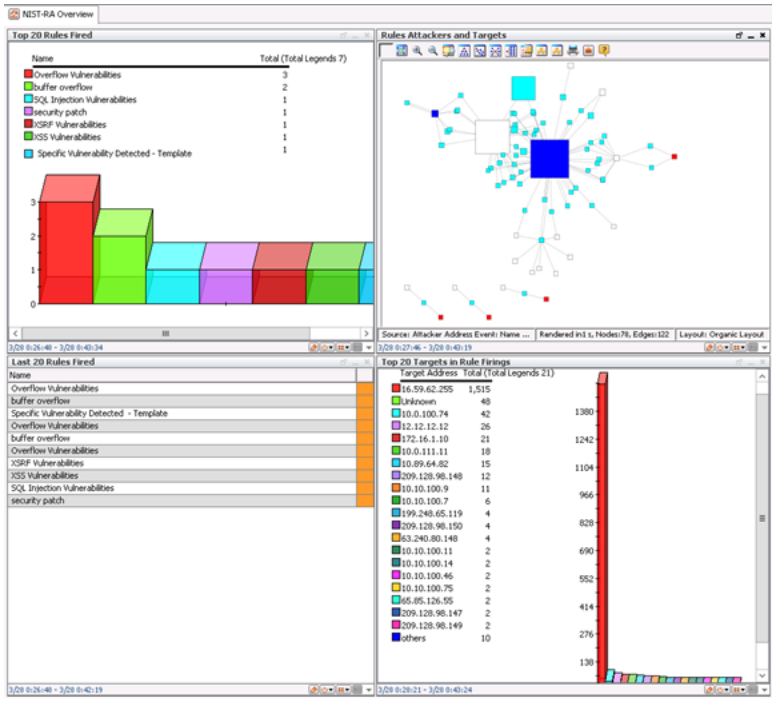
Overview dashboards summarize the compliance state determined by correlation rules for each NIST 800-53 control families. The overview dashboards are available from the FISMA/Overview group as shown in the following figure:



Each dashboard presents:

- An event graph that shows the relationships of the non-compliant systems with others on the network.
- A list of the last 20 triggered rules.
- A pie chart that breaks down the percentage of each triggered rule.
- A bar chart that shows the top 20 targets of the triggered rule.

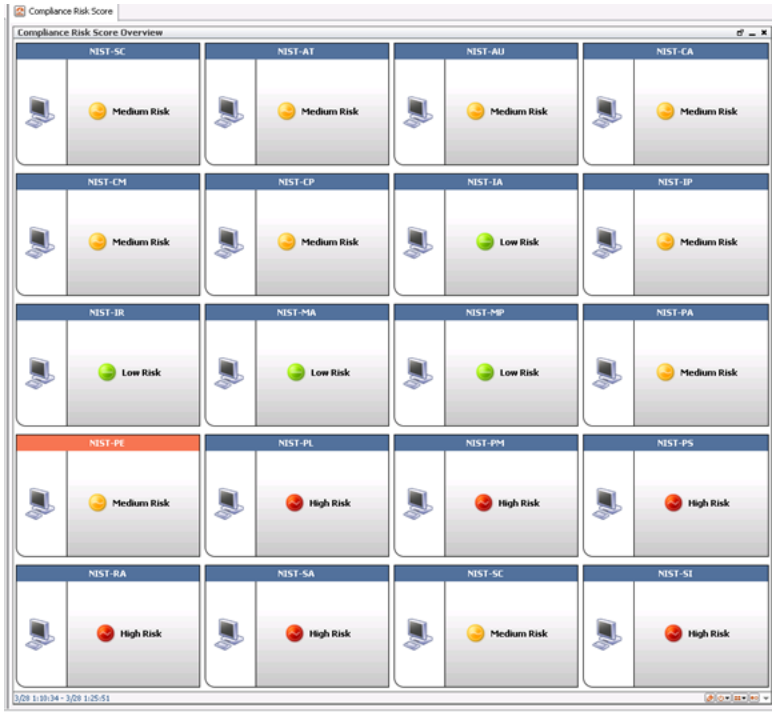
The following figure shows the NIST-RA Overview dashboard:



Risk Score Overview Dashboard

In addition to the overview dashboards, FISMA for ESM provides Compliance Risk Score dashboard which offers a high-level overview of the risk associated with each NIST family of the NIST 800-53 standard in your environment.

The Compliance Risk Score dashboard summarizes your environment's overall state of compliance with the NIST 800-53 standard as determined by correlation rules triggered for each family as shown in the following figure:



The dashboard is populated when a possible violation or an actual violation occurs. A yellow or red data monitor can be manually turned to green when the situation is remedied by right-clicking the data monitor and selecting Override Status.

The colors of the traffic lights indicate the current state as described in the following table:

Color	State	Description
Red	Violation	This situation occurs when one or more rules are triggered by event activity that violates compliance for this NIST 800-53 Security rule section
Yellow	Possible Violation	This situation occurs when one or more marginal events occur that could indicate a policy problem, or is a borderline compliance violation
Green	Compliant	Systems are considered compliant when any events related to this HIPAA Safeguard Remain under the threshold of Yellow.

Before running the Compliance Risk Score dashboard make sure the following:

- Data monitor Compliance Risk Score Overview which available also from FISMA/Overview should be enabled.
- Rule Compliance Score Update which available also from FISMA/Overview should be enabled and deployed.
- Rule Manual Status Change which available also from FISMA/Overview should be enabled and deployed.

Notify, Investigate, Analyze, and Remediate

Once a security or compliance-related activity is identified, FISMA offers many ways to take action, investigate, and analyze:

Notifications

The first step in any escalation process is to notify the right people of a potential problem. In FISMA, you can activate your notification hierarchy in case of certain threats by notifying the right groups in each situation.

Cases

Cases are ArcSight's built-in trouble-ticket system. When certain compliance-related conditions occur, FISMA can be configured to open a case to track an issue so it can be investigated and properly remediated.

ArcSight Activate

The ArcSight Activate Framework is a modular, end-to-end content development method designed to quickly deploy actionable security use cases. ArcSight Solution for FISMA provides an option to ingest FISMA rules outputs into ArcSight Activate actionable outputs. See "Configure FISMA Rules for ESM to work with ArcSight Activate Framework" on page 49.

Solution for FISMA CIP Device Coverage

Solution for FISMA CIP leverages event feeds from multiple sources. For a list of devices that are capable of generating events to populate the CIP for FISMA reports and other resources, see "CIP for FISMA Use Cases" on page 50.

To gather events from physical access devices, such as badge readers, you must build FlexConnectors tailored to the type of physical access device you use. For instructions about how to build and configure a FlexConnector for a physical access device, see "Build FlexConnector(s) for Physical Access Devices" on page 47.

Chapter 2: Solution Installation and Configuration

This chapter contains information on installing and configuring the Compliance Insight Package for FISMA 6.0 (CIP for FISMA).

Prepare for Installation

Before installing CIP for FISMA, complete the following preparation tasks:

1. "Prepare Environment" below
2. "Verify Environment" below

Prepare Environment

Before installing, prepare your environment for the CIP for FISMA:

1. Install and configure the appropriate SmartConnectors for the devices found in your environment.

   Note: The devices that provide events for the CIP for FISMA reports are listed in "CIP for FISMA Use Cases" on page 50.

2. Model your network to include devices that supply events that help satisfy the FISMA Requirements. Verify that zones and networks are defined for your environment and that networks are assigned to the connectors reporting FISMA-relevant events into your ArcSight Manager. Learn more about the ArcSight network modeling process in *ArcSight ESM 101*. Find instructions for how to configure zones and networks in the *ArcSight Console User's Guide* or the *ArcSight Console User's Guide* online help.

   Note: RFC 1918 addresses (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) are automatically categorized as protected because their zones already are categorized as protected.

Verify Environment

Before installing, verify your ArcSight ESM installation. Compliance Insight Package for FISMA is supported on ArcSight ESM expect this to be 6.8.1 or later. Refer to the ESM Support Matrix for operating system requirements. Refer also to the applicable release notes.

Verify that your system has the supported ArcSight Console connected to the Manager.

Note: CIP for FISMA is a self-contained solution that does not rely on any other ArcSight solution. You can install CIP for FISMA alongside other solutions on the same ArcSight Manager. Before

installing new solutions, Micro Focus recommends that you back up any existing solutions installed on the Manager. For detailed instructions, see "Compare, Backup and Uninstall Package " on page 418.

Updating from CIP for FISMA 5.0 to CIP for FISMA 6.0 requires :

1. Back up the old solution installed on the Manager, see "Compare, Backup and Uninstall Package " on page 418.
2. Uninstall CIP for FISMA 5.0.
3. Install CIP for FISMA 6.0.

Install Solution for FISMA CIP

The solution is supplied in a single ArcSight package bundle file called ArcSight-ComplianceInsightPackage-FISMA.6.0.<nnnn>.arb, where <nnnn> is the 4 character build number.

To install the CIP for FISMA package:

1. Using the login credentials supplied to you, download the CIP for FISMA bundle from the software download site to the machine where you plan to launch the ArcSight Console:

```
ArcSight-ComplianceInsightPackage-FISMA.6.0.<nnnn>.arb
```

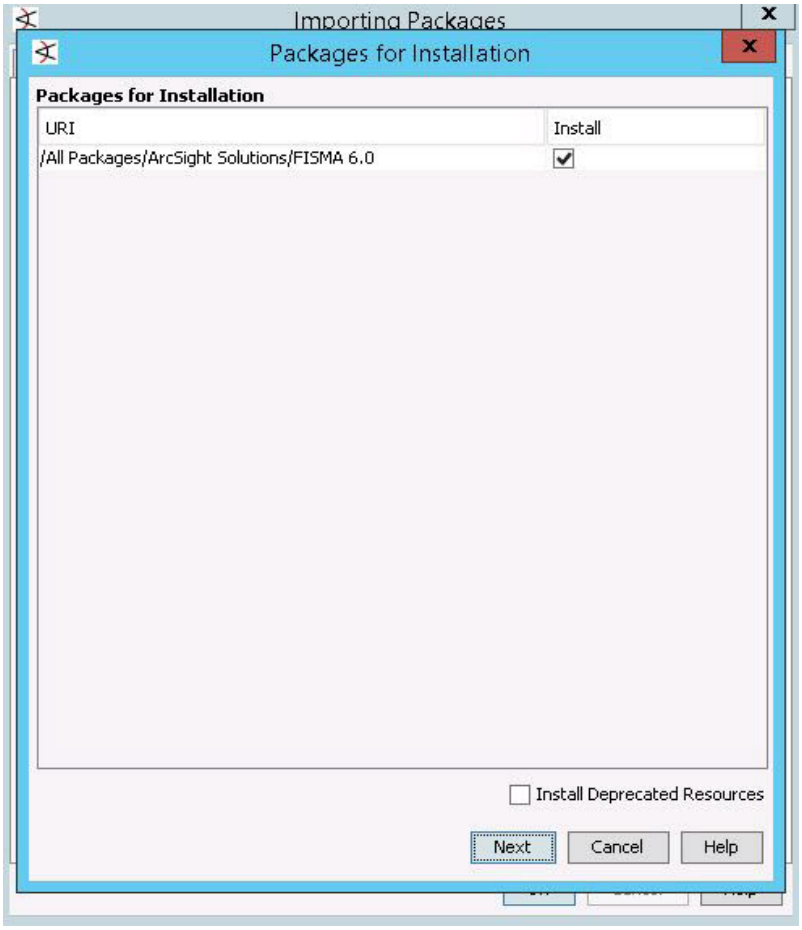
Where <nnnn> is the 4 character build number. (The exact build number is specified in the *ESM CIP for FISMA Release Notes*.)

Caution: If you use Internet Explorer to download the ARB file, it may convert the ARB file to a ZIP file. If this occurs, rename the ZIP file back to an ARB file before importing.

2. Log into the ArcSight Console as an ArcSight Administrator.
3. Click the **Packages** tab in the Navigator panel.
4. Click **Import** ( ).
5. In the Open dialog, browse and select the package bundle file and select **Open**.

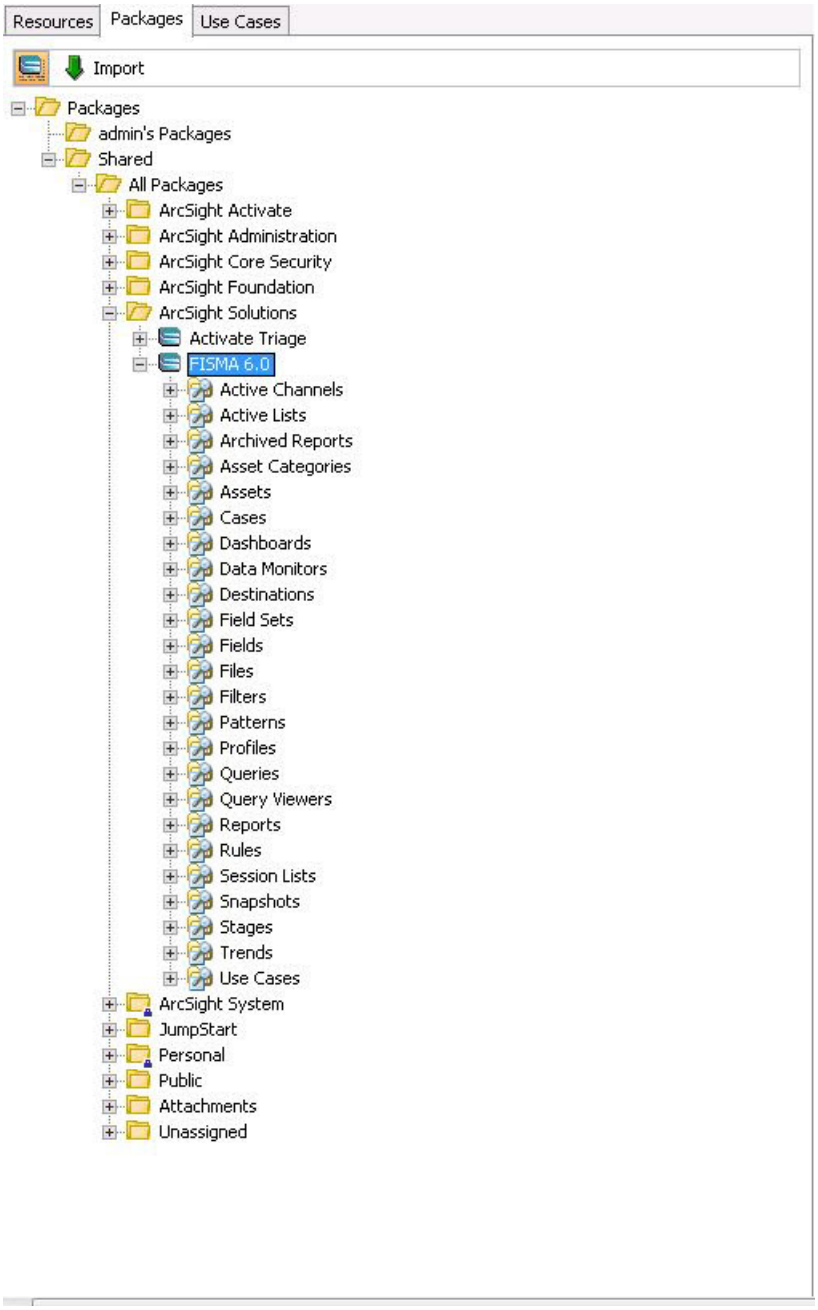
   The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

   When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog as shown in the following figure.



6. Leave the `FISMA 6.0` checkbox selected and in the Packages for Installation dialog, click **Next**.

   The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.
7. In the Installing Packages dialog, click **OK**.
8. In the Importing Packages dialog, click **OK**.
9. To verify that the installation was successful and the content is accessible in the Navigator panel, expand the `ArcSight Solutions/FISMA 6.0` group.



Assign User Permissions

By default, users in the `Default` user group can view CIP for FISMA content, and users in the `ArcSight Administrators` and `Analyzer Administrators` user groups have read and write access to the solution content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following process assumes that you have user groups set up and users assigned to them.

In the following procedure, assign user permissions to all the following resource types:

- Active channels
- Active lists
- Cases
- Dashboards
- Data monitors
- Field Sets
- Filters
- Queries
- Reports
- Rules
- Session Lists
- Trends
- Stages

To assign user permissions:

1. Log into the Console as ArcSight Administrator.
2. For all the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type and navigate to `ArcSight Solutions/FISMA`.
   b. Right-click the **FISMA** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
   c. In the ACL editor in the Inspect/Edit panel, select which user groups you want to have permissions to the CIP for FISMA resources and click **OK**.

Configure CIP for FISMA Solution

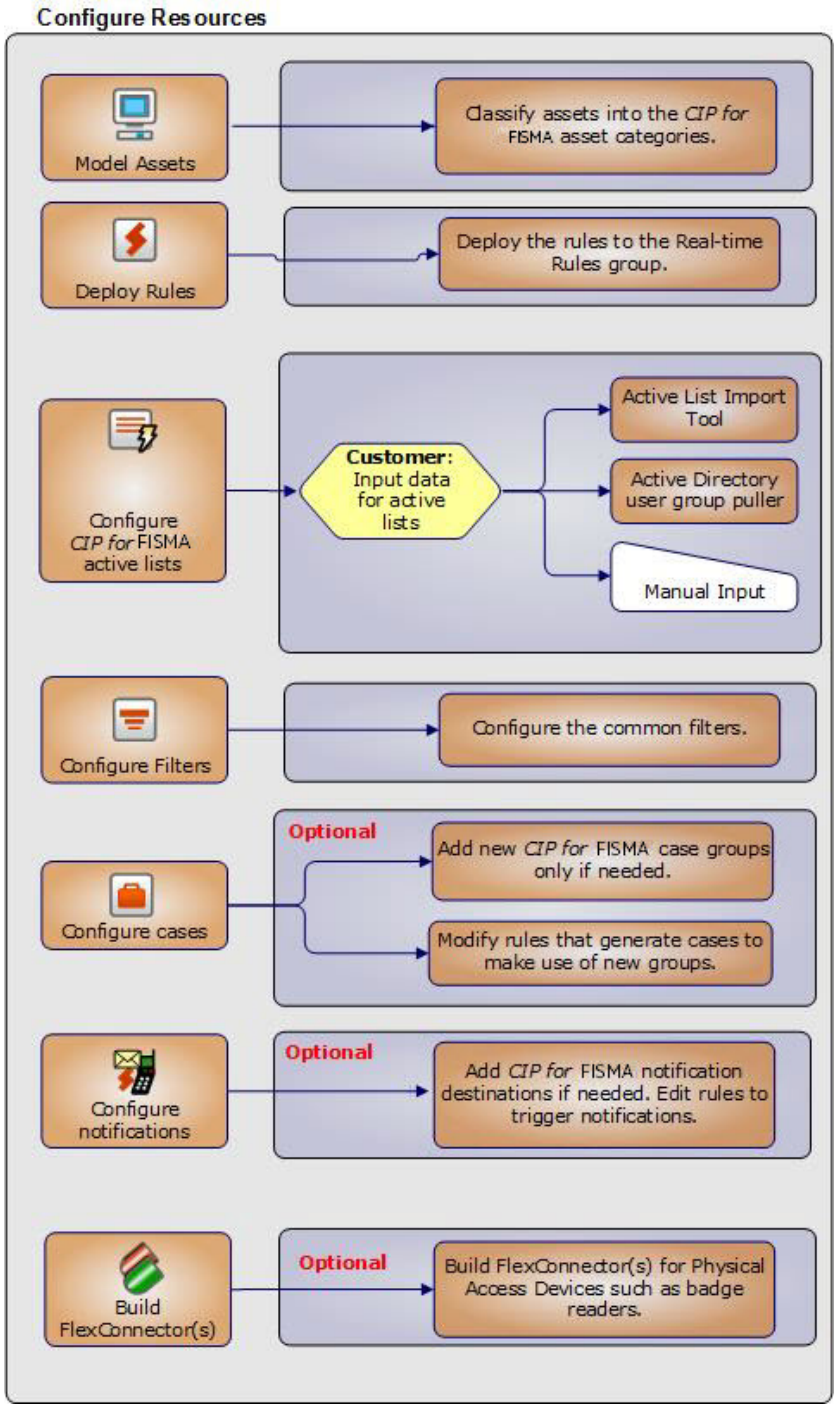
Several of the CIP for FISMA resources should be configured with values specific to your environment. Some features also require some additional SmartConnector configuration. This section describes these configuration processes.

Depending on the features you want to implement and how your network is set up, some configuration is required and some are optional. The list below shows all the configuration tasks involved with the CIP for FISMA and where to find instructions for performing the configuration.

This section contains the instructions required to enable content for the CIP for FISMA and contains the following topics:

- "Model Assets (Assign Asset Categories)" on page 22
- "Configure Active Lists" on page 24

The configuration processes outlined in this section (shown in the following figure) apply to resources that feed the CIP for FISMA.



Model Assets (Assign Asset Categories)

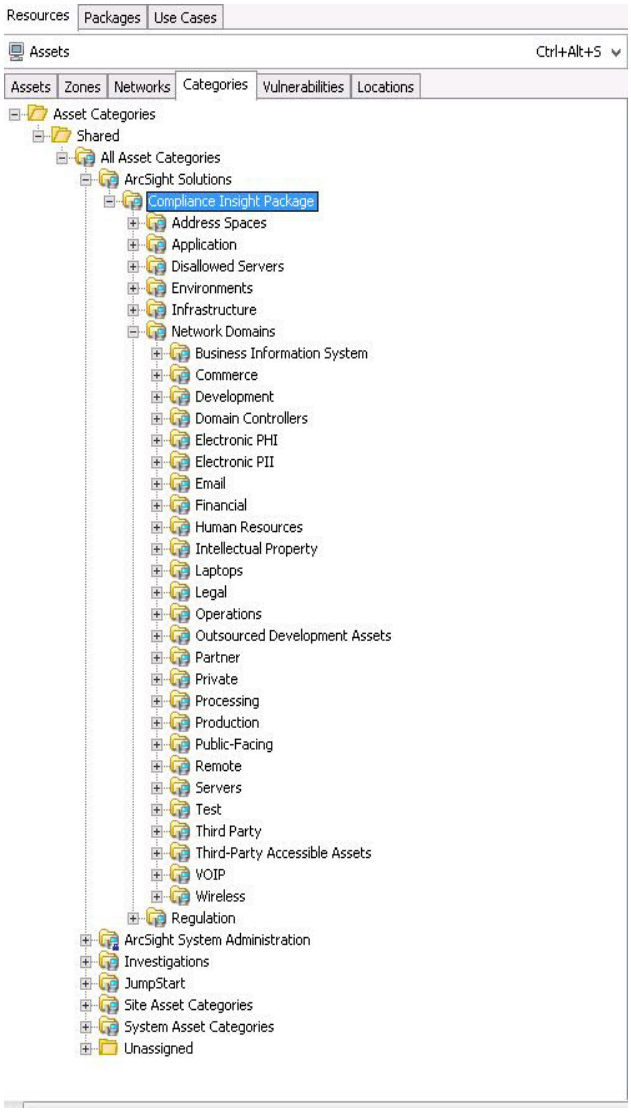
Asset modeling is essential to enable *CIP for FISMA* content. Classifying assets in one or more of the solution asset categories is essential for the following reasons:

- Some of the *CIP for FISMA* content requires assets to be modeled in order to function correctly.
- In some cases, modeling assets adds valuable business context to the events evaluated by the *CIP for*

FISMA.

CIP for FISMA Categorization

CIP for FISMA uses the asset categories under the `/ArcSight Solutions/Compliance Insight Package/` group shown below.



Categorizing Assets and Zones

CIP for FISMA solution relies on ArcSight asset and zone categorization to define your environment. Certain content does not display unless assets or zones are categorized. For detailed information about which assets and zones need to be categorized for each resource, refer to "Appendix A: CIP for FISMA Resource Reference" on page 103.

- For a list of all use cases and which assets and zones need to be categorized for each use case refer to "CIP for FISMA Use Cases" on page 46.
- For a list of all categorization used and the resources which use those categorizations, see "Appendix B: Asset and Zones Categories" on page 104.

You can assign the solution asset categories with the following methods:

One-by-one using the ArcSight Console

Use this method if you have only a few assets to categorize. One asset can be categorized in more than one asset category. To categorize your assets one-by-one:

1. In the Navigator panel, go to **Assets** and select the **Assets** tab.
2. On the **Asset** tab, expand the groups listed.
3. For each asset you want to classify with an asset category, repeat the following steps:
   a. Right-click the asset you want to categorize and select **Edit Asset**.
   b. In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen to select new resources.
   c. In the Asset Categories Selector pop-up window, navigate to the appropriate network domain category and click **OK**.

After you assign your assets to the CIP asset categories, you can also assign them to other asset categories, either within the solution package or the general ArcSight categories, or those you have created yourself.

Using the Network Model Wizard

A Network Model wizard is provided on the ArcSight Console (menu option **Tools > Network Model**). The Network Model wizard enables you to quickly populate the ESM network model by batch loading asset and zone information from comma-separated value (CSV) files. For more information, see the ArcSight Console User's Guide.

Using the ArcSight Asset Import File Connector

If you have many assets that you want to track, you can configure them in a batch using the ArcSight Asset Import File Connector. This connector can also create new assets as part of the batch function. The ArcSight Asset Import File Connector is available as part of the ArcSight SmartConnector download. For instructions on how to use this connector to configure your assets for CIP FISMA, see the *ArcSight Asset Import File SmartConnector Configuration Guide*.

Configure Active Lists

CIP for FISMA contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters, rules, and

reports.

You can populate the FISMA active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight Console. For detailed instructions, see "Configure Active Lists Using Console Active List Editor" on page 29. This method can be used to populate active lists with one, two, or more columns.
- Add entries in batch to active list from a comma separated value (CSV) file. For detailed instructions see "Configure Active Lists by Importing a CSV File" on page 29. This method can be used to populate active lists with one, two, or more columns.

Active Lists Requiring Configuration defines the active lists that require configuration for the CIP for FISMA. Some active lists are intended to be populated by rules. Also, there are Active Lists requiring manual Configuration for the CIP FISMA. For a complete listing (with descriptions) of all active lists provided with CIP for FISMA, see "Active Lists that Require Configuration" below.

Active Lists that Require Configuration

Active List	Description	Expected Input Per Entry
Active Directory Domains	This active list contains all the AD domains. This list is used on different scenarios like detecting when user account is deleted, enabled, disabled or special privileged assigned to new logon, domains should be provided on lowercase.	Active Directory Domain , in lowercase
Administrative Accounts	This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure. This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".	User name, in lowercase.

Allowed Ports	This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy. By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.	Connection type and port number Where Connection type could be: Inbound, outbound or internal
Badges to Accounts	This list contains the computer account and employee type for every physical device badge. Populate this active list with the badge ID, primary computer account for the badge holder (in case it's a visitor use the visitor user name), and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the word "Contractor", "Visitor" (case insensitive) in the employee type field.	Badge ID, primary computer account for the badge holder (in case it's a visitor use the visitor user name), the employee type (in lowercase). Specifically, ensure that Contractors and visitors are identified with the word "Contractor" "Visitor" (case insensitive) in the employee type field.
Competitors	This list stores competitor email domains on lower case, for example if the user email format of your competitor is jsmith@example.com then the email domain in this example is "example.com" (what after the @ in lowercase).	Competitor email domains on lower case.
Default Vendor Accounts	This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.	Default user account and vendor name, in lowercase.

Disallowed Ports	This active list contains all disallowed destination ports. This active list should be populated according to your site policy. By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.	Connection type and port number Where Connection type could be: inbound, outbound or internal
DMZ Assets	This List should contains DMZ assets on the organization like DNS,WEB,SMTP servers. It contains 2 fields : IPAddres and AssetType where the IPAddress is the IP Address of the asset and the AssetType is the type of the asset on lower case (by default supported 3 types dns,web,smtp). For example if your web server ip is x.y.z.w you should add it as IPAddress=x.y.z.w ,AssetType=web	IP Address of authorized DNS,WEB, SMTP servers on your organization, Asset Type one of the following dns, web smtp on lower case.
Former Employees	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.	This list populated by the rule “Former Employee Account Detected”, if this rule is disabled and not deployed this list should be maintained on regular basis and username should be provided on lowercase.
Important Emails	This list stores important emails of high-profile targets on the organization like C-lever executives which could be targeted by spear phishing attacks. entries in this list should be in all lower case.	Email and UserName , in lowercase
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Port Number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Process name, in lowercase
Internet Ports	This active list includes ports that are used for monitoring internet (Web traffic) communication. By default, it includes ports 80 and 443.	Port Number

Meltdown and Spectre Signatures	This active list contains Meltdown and Spectre vulnerabilities signatures.	This list should be maintained on a regular basis.
Mobile Code Detection Signatures	This active list contains a list of mobile code detection signatures.	This list should be maintained on a regular basis.
Monitored Accounts	This active list is used to maintain user accounts to be monitored.	Usernames in lowercase
Monitored FISMA Reports	This active list is updated when a monitored FISMA report is accessed. Before enabling and deploying those rules : 1. FISMA Report Accessed 2. FISMA Report not Accessed more than x days Make sure to populate this active list with the reports that you want to monitor. For example if you want to monitor this report : /All Reports/Arcsight/Solution/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins Please add the following entries to the active list : Report : /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins	FISMA Report URI
Multi Factor Authentication Devices	This active list stores the multi factor authentication devices, All the entries in this list must be in lowercase.	Device product, device vendor and device version on Lower case
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	User Name, in lowercase. This list should be maintained on a regular basis.
Non Multi Factor Authentication Devices - Exception	This active list stores non multi factor authentication devices which you want to exclude, All the entries in this list must be in lowercase.	Device product, device vendor and device version on Lower case

Test and Custom Accounts	This active list stores names of development, test, or custom application or user accounts. Populate this active list with additional custom accounts that should be disabled in a production environment. All the entries in this list must be in lowercase.	Account Name, in lowercase. This list should be maintained on a regular basis.
Unsecured Password Signatures	This active list contains unsecured password signatures.	This list should be maintained on a regular basis.
Users Authorized to Access High Impact Systems	This active list stores the usernames of the individuals who are authorized to access high impact systems. All the entries in this list must be in lowercase.	Username, in lowercase
VOIP Applications Detection Signatures	This active list contains a list of voip applications signatures.	This list should be maintained on a regular basis.

Configure Active Lists Using Console Active List Editor

You can add entries to active lists, one-by-one, using the Active List editor of the ArcSight Console.

1. In the Navigator panel, go to Lists and navigate to `ArcSight Solutions/FISMA`.
2. Right-click the active list you wish to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
3. For each entry you wish to add to the active list, repeat the following steps:
   a. To add an entry to the list, click the add icon ( ) in the active list header.
   b. In the Active List Entry editor of the Inspect/Edit panel, enter values for each column in the list except for the dynamic columns listed in the following table and click **Add**.

Name	Value
Creation Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Last Seen Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Count	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field unchanged.

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For

example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

1. In the Active Lists resource tree of the ArcSight Console, right-click an active list and choose **Import CSV File**.

   A file browser opens.
2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, in the Import Preview dialog, click **OK**. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

   This displays the newly-added data from the CSV file in the Viewer panel as active list details.

   Tip: By default, the active list displays 2000 entries at a time. To view entries outside the range shown, create an active list filter that specifies a different range (click **Filter** in the active list header).

Configure My Filters

Configure the following common filters stored in the `My Filters` group to reflect your organization:

- "After Hours Filter" below
- "Limit Regulation Filter" on the next page

After Hours Filter

The After Hours filter defines the time period which is considered to be after business hours. The default after hours time period is set to 8:00 p.m. to 6:00 a.m. on weekdays, and all day Saturday and Sunday.

The filter uses two variables:

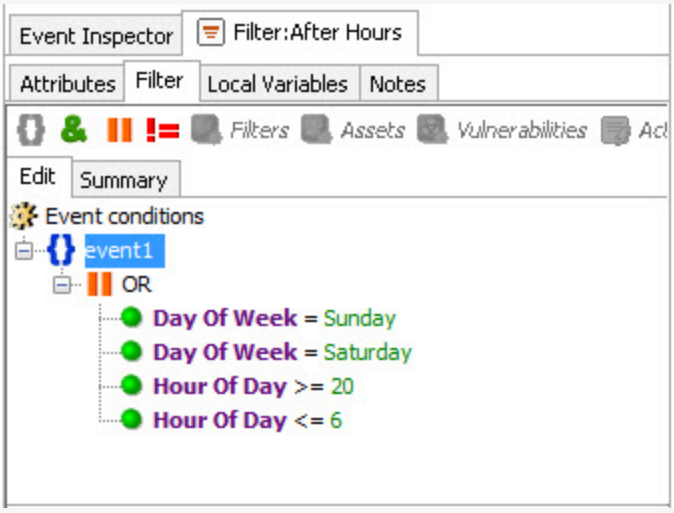
- `DayOfWeek`
- `HourOfDay`

You can change this filter to match what is considered to be after hours for your organization.

Tip: The `DayOfWeek` variable returns an integer value that is displayed on the ArcSight Console as a string value of the current day: `Saturday`, `Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, or `Friday`. Since the `DayOfWeek` variable is an integer, you can specify a range of days such as (DayOfWeek >= Monday AND DayOfWeek <= Friday).

The HourOfDay variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23.

For example, to redefine the after business hours from 6:00 PM to 8:00 AM on all weekdays and all of Saturday and Sunday use the filter show in the following figure.



Limit Regulation Filter

The Limit Regulation filter limits event processing to only those events addressed by the FISMA regulation. Customize it to reflect your environment.

For example, you could configure it to specify the following conditions:

- The source machine is an asset under the FISMA
- The source machine's zone is categorized as FISMA
- The destination machine is an asset categorized as FISMA
- The destination machine is an asset under the FISMA group
- The destination machine's zone is categorized as FISMA
- The device machine is an asset categorized as FISMA
- The device machine is an asset under the FISMA group
- The device machine's zone is categorized as FISMA

By default, the CIP for FISMA processes all incoming events.

Deploy the CIP for FISMA Rules

In order for the CIP for FISMA to process FISMA-related events, the solution rules have to be deployed to the `Real-time Rules` group. By default, CIP for FISMA rules are not deployed in the `Real-Time Rules` group because deployed rules can have a performance impact. Only deploy a rule into the

Real-time Rules group if you are interested in the associated use case and have device feeds configured in your environment that can trigger the rule.

To deploy a rule:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSight Solutions/Rules group.
2. Expand the FISMA folder that contains the rule to deploy and select the rule. For example, to select the **Potential Ransomware Activity on Critical Windows Machine** rule, expand /Arcsight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmware,and Information Integrity..
3. Drag and drop the selected rule from the appropriate /ArcSight Solutions/FISMA group into the Real-time Rules/FISMA group.
4. From the Drag & Drop Options dialog, select the **Link** option.

The rule is listed under the `Real-time Rules/FISMA` group as shown in the following figure.

The rule in the `Real-time Rules/FISMA` group is a link to the rule in the `ArcSight Solutions/FISMA` group.

Note: By default, the CIP for FISMA rules are disabled. The rules do not trigger until they are

deployed and enabled. After you have deployed the CIP for FISMA rules to the Real-time Rules group, you can enable individual rules. Rules can place an additional load on the ArcSight Manager. Enable only the rules for the compliance scenarios you want to implement.

To enable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the `Real-time Rules/FISMA` group.
2. Navigate to the rule you want to enable.
3. Right-click the rule and select **Enable Rule**. To select multiple rules, press the **Ctrl** key and click each rule. To select a range of rules, press the **Ctrl** and **Shift** keys and click the first and last rule in the range.

Certain use cases in the CIP for FISMA require that specific rule actions be enabled to trigger actions in the system, such as the creation of a new case. To enable a rule action, select an action below a trigger in the Actions tab of the Rule Editor and click **Enable Action**.

For more information about working with rules, see the *Rules Authoring* topic in the *ArcSight Console User's Guide*.

Enable Data Monitors

All of the CIP's data monitors for FISMA must be enabled to display data in the dashboards that use them.

To enable the data monitors:

1. In the Navigator panel, go to **Dashboards** and click the **Data Monitors** tab.
2. Navigate to the `/All Data Monitors/ArcSight Solutions/FISMA` group.
3. Right-click the CIP group and select **Enable Data Monitor** to enable all the data monitors in the group.

Enable and Test Trends

By default, trends included in the CIP are not enabled. Some reports, query viewers, and dashboards require enabled trends to show data.

Before enabling a trend, verify that the trend captures data relevant for your environment as described in the procedure below:

1. Generate or identify the required events and verify that they are being processed by ArcSight ESM.
2. Navigate to the appropriate trend, right-click the trend, and then choose **Test**. If you see the events of interest in the test panel, then ArcSight ESM is processing events that can be captured by the trend. The test panel shows relevant events that can be captured by the trend in the last hour, up to 25 rows.

In addition, before enabling a trend, you can also customize its values like `Partition Retention Period (in days)` and `Scheduler Start Time`.

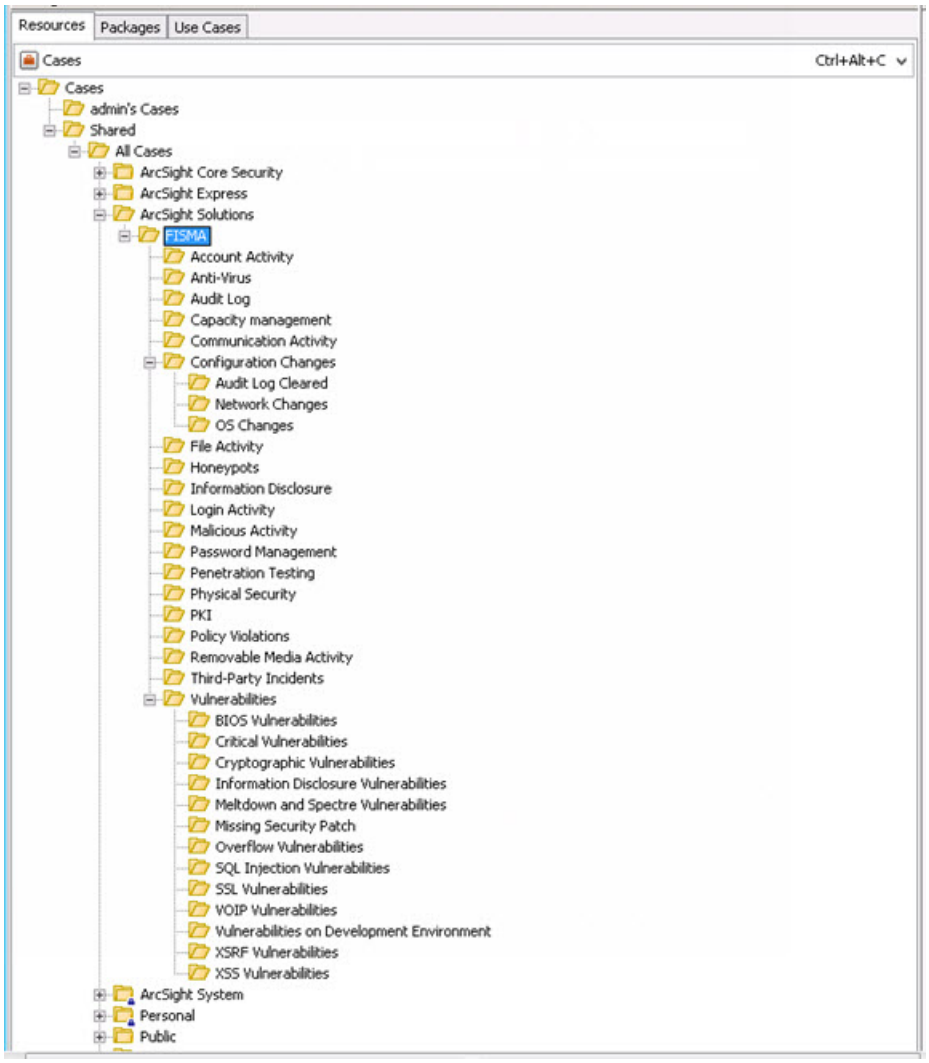
For general information about trends, see:

- *ArcSight Console User's Guide*
- *ESM Best Practices: Trends*

See "Compare, Backup and Uninstall Package " on page 418 for a list of reports, query viewers, and dashboards that use trends to display data.

Configure Cases

Cases are ArcSight's trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. FISMA for ESM includes the `ArcSight Solutions/FISMA` group, which holds the cases generated by some FISMA rules.



You can add more groups to the `ArcSight Solutions/FISMA` group or your own group if you want to add more differentiations. If you do add more groups to the `ArcSight Solutions/FISMA` group, modify the ESM rules that generate cases to use of your new case groups.

The rules listed below can generate cases by default in the FISMA directory.

Rule Name	Rule URI	Case URI
ASLR or Data Execution Prevention Bypass Flaw on Critical Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities
After Hours Building Access by Contractors	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Attacks Against Organization Increased Exponentially in less than 10 Minutes	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Attempted File Changes in Development Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/File Activity
Audit Log Cleared	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-9 Protection of Audit Information/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/Audit Log Cleared
BIOS Flaws	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/BIOS Vulnerabilities
Command Injection on HTTP Request	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Communication between Non Classified Machines and Classified Machines Domains	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Cases/All Cases/ArcSight Solutions/FISMA/Communication Activity
Communication between Production and Development Domains	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Cases/All Cases/ArcSight Solutions/FISMA/Communication Activity
Communication between Sensitive Asset and Test Domain	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Cases/All Cases/ArcSight Solutions/FISMA/Communication Activity

Communication between Sensitive Asset and Third Party Domain	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Cases/All Cases/ArcSight Solutions/FISMA/Communication Activity
Consecutive Unsuccessful Logins to Administrative Account	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
Consecutive Unsuccessful Logins to Monitored Account	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
Critical Change on Production Environment	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes
Critical Network Device Configuration Change Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/Network Changes
Critical Operating System Change Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Critical Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Critical Vulnerabilities
Cryptographic Hash Algorithm Related Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
Cryptographic Public Key Related Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
Cryptographic Symmetric Key Related Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
Cryptographic Weak Protocol Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
DNS Abnormal Queries Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity

Data Execution Prevention (DEP) is Disabled on Critical Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Disabled User Account Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Disallowed Ports Access	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
DoS Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Email Sent from High Profile User to Competitor Company	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Enabled User Account Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Encrypted Communication Information Leaks	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Information Disclosure
Excessive Blocked Firewall Traffic from the same Source	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Excessive SIP 4XX Response	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/VOIP Vulnerabilities
FISMA Report not Accessed more than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-5 Response to Audit Process Failure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Audit Log
Failed Access by the Same User to Multiple Buildings	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Failed Anti-Virus Updates	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	/All Cases/All Cases/ArcSight Solutions/FISMA/Anti-Virus

Failed Building Access	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Failed Virus Removal Attempt	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Anti-Virus
Former Employee Account Activity	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Former Employee User Account Access Attempt	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Frequent Unsuccessful Logins by User Name to Multiple PII Assets on Short Period	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
Hacker Tool Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
High to Low Classified Traffic Information Leak	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Cases/All Cases/ArcSight Solutions/FISMA/Communication Activity
Inactive User Account Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Information Disclosure Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Information Disclosure Vulnerabilities
Insecure Cryptographic Storage Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
Insider Threat Against Single Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Insider Threat Increased Exponentially in less than 10 Minutes	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Internal Recon Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity

Invalid or Expired Certificate	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	/All Cases/All Cases/ArcSight Solutions/FISMA/PKI
Local Logon from Badged Out Employee	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Login Activity by a Stale Account	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Meltdown|Spectre Vulnerability Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Meltdown and Spectre Vulnerabilities
Minimum Password Age Changed to Less than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Password Management
Minimum Password Length Changed to Less than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Password Management
Multiple Policy Violations Against Assets Categorized with the Same Network Domains	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Cases/All Cases/ArcSight Solutions/FISMA/Policy Violations
One or more Rows have been Deleted from the Certificate Database	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	/All Cases/All Cases/ArcSight Solutions/FISMA/PKI
Organizational Data Information Leak	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Information Disclosure
Overflow Vulnerabilities	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Overflow Vulnerabilities
Password Spray Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Password Management
Password not Changed for Longer than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Password Management

Penetration Testing not Performed for Longer than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 8 Penetration Testing/	/All Cases/All Cases/ArcSight Solutions/FISMA/Penetration Testing
Personal Information Leak	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Information Disclosure
Possible Botnet Activity	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Covert Channel	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-31 Covert Channel Analysis/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible DNS Based Zombie	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible DNS Tunneling	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Email Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible HTTP Based Zombie	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Information Interception	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Redirection Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible SMTP Based Zombie	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Spam Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Possible Spear Phishing Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity

Possible Traffic Anomaly	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Potential Badge Cloned	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Potential Distributed DoS	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Potential Email Bomb Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Potential Piggybacking Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Physical Security
Potential Ransomware Activity on Critical Windows Machine	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Cases/All Cases/ArcSight Solutions/FISMA/File Activity
Potential Worm Propagated Internally	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Privileged Account Changes	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Recon Activity from the Same Country Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Removable Media Activity by Non Identifiable Account	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	/All Cases/All Cases/ArcSight Solutions/FISMA/Removable Media Activity
Removable Media Detected on Highly Critical Machine	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Cases/All Cases/ArcSight Solutions/FISMA/Removable Media Activity
Removable Media Plugged In Multiple Assets in Short Period of Time	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	/All Cases/All Cases/ArcSight Solutions/FISMA/Removable Media Activity

Resource Exhaustion Detected on Critical Machine	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-4 Audit Storage Capacity/	/All Cases/All Cases/ArcSight Solutions/FISMA/Capacity management
Rogue Station Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
SQL Injection Vulnerabilities	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/SQL Injection Vulnerabilities
SSL|TLS Vulnerabilities on Public Facing Assets	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Cryptographic Vulnerabilities
Same User Using Different User Names to Login	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
Security Log is Full	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-5 Response to Audit Process Failure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Capacity management
Security Patch Missing	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Missing Security Patch
Service Installed on Critical Windows Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Severe Information Disclosure Vulnerability on PII Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Information Disclosure Vulnerabilities
Severely Attacked System	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Severely Attacked System Originated from Third Party Assets	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Shell Code Execution Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Shutdown Machine not Started more than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes

Shutdown of Highly Critical Machine	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Shutdown of Multiple Machines on Production Environment on Short Period of Time	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Special privileges assigned to new logon	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 6 Least Privilege/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Specific Vulnerability Detected - Template	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities
Spyware Detected on Critical Asset	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Successful Attack - Brute Force Login	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
Successful Non VPN Remote Access	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Suspicious Activities by Former Employee	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Suspicious Activities by New Hires	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	/All Cases/All Cases/ArcSight Solutions/FISMA
Suspicious Activities by a Stale Account	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
System Shutdown or Restart at Unscheduled Time	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Targeted Recon Activity from the same Country against Multiple PII Assets	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Unable to Log Events to Security Log	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-5 Response to Audit Process Failure/	/All Cases/All Cases/ArcSight Solutions/FISMA/Capacity management

Unauthorized Access to High Impact Systems	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	/All Cases/All Cases/ArcSight Solutions/FISMA/Account Activity
Unscheduled Change in Status of Service	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes/OS Changes
Unsecured Password Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	/All Cases/All Cases/ArcSight Solutions/FISMA/Password Management
Unsuccessful Logins to Multiple Administrative Accounts	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
User Logged in from Two Countries	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
User Logged in from different IP Addresses	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Cases/All Cases/ArcSight Solutions/FISMA/Login Activity
VOIP Ghost Call Attack	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/VOIP Vulnerabilities
VOIP Vulnerabilities	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/VOIP Vulnerabilities
Vulnerabilities on Critical Machine	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Critical Vulnerabilities
Vulnerabilities on Development	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/Vulnerabilities on Development Environment
Vulnerability Scanner didnλ€™t Run for Longer than Policy Standard	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities
Windows Domain Policy Changed	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	/All Cases/All Cases/ArcSight Solutions/FISMA/Configuration Changes

Wireless Malicious Traffic Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
Worm Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	/All Cases/All Cases/ArcSight Solutions/FISMA/Malicious Activity
XSRF Vulnerabilities	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/XSRF Vulnerabilities
XSS Vulnerabilities	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Cases/All Cases/ArcSight Solutions/FISMA/Vulnerabilities/XSS Vulnerabilities

By default, the **Add to Existing Case** action for these rules are disabled. Enable the **Add to Existing Case** actions only for the rules that detect events that are important to your organization and therefore should be tracked with cases.

To enable the Add to Existing Case action for a rule:

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the `ArcSight Solutions/FISMA` group.
2. Right-click a rule and select **Edit Rule**.

   The rule displays in the Inspect/Edit panel.
3. Right-click the **Add to Existing Case** action, select **Enable Action** and click **Apply.**

After enabling the **Add to Existing Case** action, one of the following occurs when the rule fires:

- If a case with the same name does not exist, a new case is created.
- If a case with the same name does exist, the existing case is updated with additional events.

If you want to generate cases for additional activities, you can edit any rules in the `ArcSight Solutions/FISMA` that trigger on that specific behavior and add actions those rules to create cases. For example, if you want to create a case every time an account is locked out, edit the Configure Notifications rule and add an action that creates a case.

Caution: Use caution when adding a **Create New Case** action to a rule. Every time a rule fires, a new case is created. If you expect the rule to fire repeatedly, consider using **Add to Existing Case** action instead.

If you are using the **Add to Existing Case** action and you choose to close the case, consider the following in order to detect new issues when the same circumstances re-occur:

1. Copy the case to another location.
2. Delete the case from the original directory.

Configure Notifications

When enabled, a notification action on a rule sends a notification when the rule fires. The following rules contain notification actions that are disabled by default:

Rule Name	Rule URI
Account Lockout	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-7 Unsuccessful Login Attempts/
DHCP Critical Logging Error Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/
Multiple Cases Created on Short Period	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/
Security Software Stopped or Paused	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/
Severe Honeypot Interaction Activity Increased Exponentially in less than 10 Minutes	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/
Successful Default Vendor Account Used	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/
Suspicious Internal Trojan Detected	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/

You can enable the notification actions for these rules. You can add a rule action to other `ArcSight Solutions/FISMA` rules. In addition, you can create notification destinations that receive the notifications when the rules fire. For more information including configuration information, see the *Notifications* topic in the *ArcSight Console User's Guide*. This configuration is optional.

Configure Additional Resources

Additional configuration may be required or desired for the individual resources provided to address a specific FISMA Requirements. For more information, see "CIP for FISMA Resource Reference " on page 102.

Build FlexConnector(s) for Physical Access Devices

The Compliance Insight Package for FISMA contains resources that make use of feeds from physical access systems, such as badge readers. This process is only required if you want to activate the CIP for FISMA content that leverages feeds from physical access systems. If you do not complete this process, the content that leverages feeds from physical access systems will remain dormant.

To enable these scenarios, develop a FlexConnector according to the instructions in the *ArcSight FlexConnector Developer's Guide* with the following field mappings to map the key event data into the ArcSight event schema:

Field Mappings

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event Categories

Event type	Object	Behavior	Technique	Device Group	Outcome	Significance
Successful building access	/Location	/Authentication/Verify		/Physical Access System	/Success	/Normal
Building access rejected	/Location	/Authentication/Verify		/Physical Access System	/Failure	/Information/ Warning
Badge-out (someone is leaving a building) [not all badge reader systems support this]	/Location	/Access/Stop		/Physical Access System	/Success	/Normal
Account created/deleted/modified - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authentication/ [Add|Delete|Modify		/Physical Access System	/Success	/Informational
Giving someone access to another room/building - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authorization/Modify		/Physical Access System	/Success	/Informational
Granting access to a room/building for an entire group of users	/Actor/Group	/Authorization/Modify		/Physical Access System	/Success	/Informational

You can add more user context to the events generated by your badge reader by creating a connector event mappings file.

Configure FISMA Rules for ESM to work with ArcSight Activate Framework

1. In the Navigator panel, go to Rules and navigate to the Real-time Rules/FISMA group.
2. Navigate to the rule you want to configure.
3. Right-click the rule and select **Edit Rule.**
4. On the action tab go to **Set Event Fields Actions**. Right-click **Event Annotation Stage field**, and select **Enable Action.**

Chapter 3: CIP for FISMA Use Cases

The Compliance Insight Package for FISMA contains different use case resources. A use case resource provides a way to group and view a set of resources that help you to measure and report on compliance with the NIST 800-53 regulation safeguards.

To view the resources associated with a use case resource:

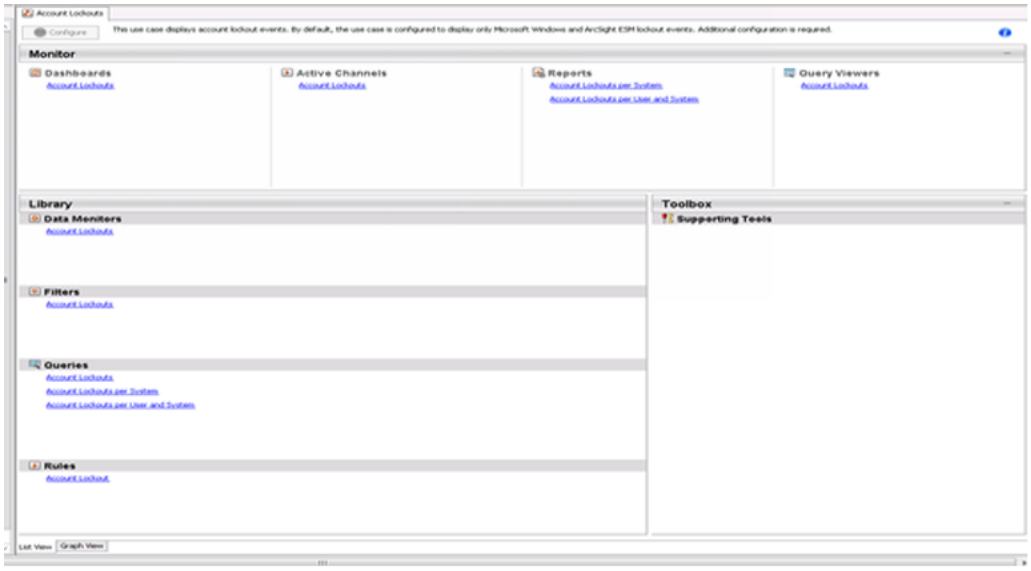
1. In the Navigator panel select the **Use Cases** tab.

2. Browse for the **Use Case** resource (such as ArcSight Solutions/FISMA/Account Lockouts).

3. Right click the use case resource and select the **Open Use Case** option.

The resources that make up a use case resource are displayed as shown in Figure 4-1. The use case resource tables listed below contain all the resources that have been explicitly assigned to the use case.

Figure 4-1 Viewing the Resources Assigned to the use case:



General Use Cases

Use Case	Description	NIST 800-53 Controls	Supported Devices	Special Configuration
ASLR and Data Execution Prevention	This use case provides information about ASLR and data execution prevention flaws.	SI-16	Vulnerability Assessments	1. Before deploying the rules please make sure assets or zones are categorized. 2. The following rule “Data Execution Prevention (DEP) is Disabled on Critical Asset” and the following report “Disabled Data Execution Prevention (DEP) Mechanism” are based by default on Nessus Plugin Nessus|24282,as mentioned on the filter : “Data Execution Prevention (DEP) is Disabled”, If you want to support another devices please make sure to reconfigure this filter. 3. Before Running this report “Weekly Report - ASLR or Data Execution Prevention Bypass Flaws”, please make sure the following trend “/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/ RA- 5 Vulnerability Scanning/Vulnerabilities” is enabled.
Accesses through AAA Server	This use case provides overview of accesses through AAA Server.	IA-3	Identity Management	
Account Additions, Deletions, and Modifications	This use case provides information about account management activities.	AC-2	Operating System	Certain content does not display unless assets or zones are categorized.

Account Lockouts	This use case displays account lockout events. By default, the use case is configured to display only Microsoft Windows and ArcSight ESM lockout events.	AC-7	Operating Systems	1. Edit the **Account Lockouts** filter to add conditions for lockout events from other devices in your environment. By default, the Account Lockouts filter identifies account lockouts on Microsoft Windows and UNIX systems. Verify that the Account Lockouts filter detects events in your environment that match the expected behavior. 2. Deploy the Account Lockout rule to the real-time rules group, and enable case and notification actions if appropriate for your organization
Administrator Logins and Logouts	This use case providesinformation about the administrative logins and logouts.	IA-2,AC20,AC-7	Operating Systems IDS/IPS Databases Firewalls Virtual Private Networks identity Management Policy Management Network Equipment Content Security Web Filtering Antivirus Physical Security Systems Wireless Applications Network Based Anomaly Detection	1. In the Administrative Accounts active list, define usernames that have administrative privileges in your environment. Entries should be lowercase only. 2. The Administrative Login Attempts filter defines the events to be processed by this use case. By default it includes events in which either the source or destination username is an administrative user defined in the Administrative Accounts active list. 3. Certain content does not display unless assets or zones are categorized.

Asset Inventory	The Software Inventory use case provides information about the assets in your environment.	CM-8,CP-2,PM5	Scanners	Certain content does not display unless assets or zones are categorized.
Assets that Failed Technical Compliance Check	This use case provides resources which helps to identify assets that failed technical compliance check.	CA-2	Vulnerability Assessments IDS/IPS	
Attacks and Suspicious Activity	This use case provides information about events that are identified as attacks or suspicious activity.	IR-6	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	1. Certain content does not display unless assets or zones are categorized 2. Verify that the Attacks and Suspicious Activity filter detects events in your environment that match the expected behavior. 3. In order for content to display data please make sure the trend Attacks and Suspicious Activities is enabled
Audit Log Cleared	This use case provides information about events that occur when an audit log is cleared or modified manually.	AU-9	Operating Systems IDS/IPS Firewalls	By default, the **Audit Log Cleared** filter returns events indicating that audit logs have been cleared on Microsoft Windows or detected by Symantec HostID systems. Edit this filter to add conditions for additional events known to indicate audit log clearing in your environment
Audit Log Failures	This use case provides overview of audit log failures.	AU-5	Operating Systems	
Authentication or Authorization Flaws	This use case provides overview of authentication or authorization flaws.	AC-14	Vulnerability Assessments	

BIOS Flaws	This use case provides information about BIOS (Basic Input Output System) flaws on the organization.	SI-7	Vulnerability Assessments	3. Before Running this report “Weekly Report - BIOS Flaws”, please make sure the following trend “/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/ RA- 5 Vulnerability Scanning/Vulnerabilities” is enabled.
Botnet Activity	This use case provides information about possible botnet activity on the organization.	SI-4	Proxy	1. Make Sure the active list : “DMZ Assets” is configured 2. Make sure the following rule “Possible Botnet Activity” is enabled and deployed before using other resources for this use case.
Brute Force Logins	This use case identifies and provides information about brute force login attempts. The brute force login attempts can either be identified by rules in this use case or by Intrusion Detection Systems.	AC-7	Intrusion Detection Systems Operating Systems Applications Identity Management Virtual Private Networks (VPN) Databases	Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. 1. Frequent Unsuccessful Logins from Attacker Host 2. Brute Force Login Attempts 3. Frequent Unsuccessful Logins to Target Host 4. Successful Attack - Brute Force Login 5. Frequent Unsuccessful Logins by User Name 6. Frequent Unsuccessful Administrative Logins from Remote System For “Frequent Unsuccessful Administrative Logins from Remote System” rule please make sure the following active list Administrative Accounts define usernames that have administrative privileges in your environment. Entries should be lowercase only.
Changes to Privilege Accounts	This use case provides overview of changes to privilege accounts.	AC-2	Operating Systems	Please make sure the following active list **Administrative Accounts** define usernames that have administrative privileges in your environment. Entries should be lowercase only.

Changes to User Accounts	This use case provides overview of changes to user accounts.	AC-2,CM-5	Operating Systems	Certain content does not display unless assets or zones are categorized.
Clock Synchronization Issues	This use case detects when events' device receipt time is greater than the connector receipt time and when there is a large offset between the end time and manager receipt time.	AU-8	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Anti-Virus Physical Security Systems Wireless Applications Network Based Anomaly Detection	The Clock Synchronization Issues use case requires the following configuration for your environment [CIS1] : In the following filters, set the time offset per your organization's policy: 1. Big Difference Between End Time and Manager Receipt Time. 2. Device Time is later than Agent Time.
Code Signing Flaws	This use case provides overview of detecting code and software signing problems.	CM-5	Vulnerability Assessments	Please make sure the rule: Code Signing Flaw Detected is enabled and deployed before running Code Signing Flaws report.

Command Injections	This use case provides information about command injection on HTTP Requests.	SI-10	Proxy	Please make sure the rule : Command Injection on HTTP Request is enabled and deployed before running Command Injection on HTTP Request report.
Configuration Changes Overview	This use case provides general information about configuration changes on your organization.	CM-3	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Anti-Virus Physical Security Systems Wireless Applications Network Based Anomaly Detection	1. Certain content does not display unless **assets** or **zones** are categorized. 2. Please make sure the following trend **Configuration Changes** is enabled and deployed.

Covert Channel Activity	This use case report on covert channel activity, such sending TCP traffic over an ICMP channel.	SC-31	Intrusion Detection Systems Intrusion Prevention Systems	Verify that the Covert Channel filter detects events in your environment that match the expected behavior.
Critical Assets	This use case provides overview of critical assets, It can be used to identify key assets to implement the business continuity process.	CP-2	Scanners	Certain content does not display unless assets or zones are categorized.
Cryptographic Hash Vulnerabilities	This use case provides an overview of cryptographic hash vulnerabilities.	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
Cryptographic Public Key Related Vulnerabilities	This use case provides overview of cryptographic public key related vulnerabilities.	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
Cryptographic Symmetric Key Related Vulnerabilities	This use case provides overview of cryptographic symmetric key related vulnerabilities.	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case
Cryptographic Weak Protocol Vulnerabilities	This use case provides overview of cryptographic weak protocol vulnerabilities	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case
DNS Activity	This use case provides overview of DNS activity on the organization, by default it based on DNS Bind.	SC-21	DNS BIND	Before deploying this rule Possible DNS Tunneling make sure this rule: DNS Abnormal Queries Detected is enabled and deployed.

Database Configuration Changes	This use case provides overview of database configuration changes.	CM-3	Databases	Verify that the “Target Asset is Database” filter detects events in your environment that match the expected behavior or edit the “Target Asset is Database” filter to add conditions relevant to your environment.
Development Environment Monitoring	This use case monitors the activity on development environment.	SA-10	Operating Systems Vulnerability Assessments Integrity Tools	1. Certain content does not display unless **assets** or **zones** are categorized.
Disabled User Accounts	The purpose of this use case is to identify disabled user accounts.	AC-2	Operating Systems (Windows)	1. Adding the organizational active directory Domains to Active Directory Domains Active List. 2. Before running this report Disabled Privilege Accounts. Please make sure the following active list Administrative Accounts defines usernames that have administrative privileges in your environment. Entries should be lowercase only.

Disallowed Ports	This use case provides information about connections to non-allowed ports.	AC-17	Intrusion Detection Systems Intrusion Prevention Systems Firewalls Virtual Private Networks (VPN) Network Equipment Wireless	The Disallowed Ports use case supports three separate policies for port control depending on the direction of the monitored connection: inbound, outbound, or internal, as indicated in the Connection Type field of the Allowed Ports and Disallowed Ports active lists. These active lists serve as a “whitelist” and “blacklist” of ports to provide more configuration flexibility. By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list. Conditions are located in the Disallowed Ports Access filter.
DoS Activity	This use case provides overview of Denial of Service activity on the organization.	SC-5	Network Equipment Intrusion Detection Systems Intrusion Prevention Systems Firewalls Network Based Anomaly Detection Content Security Web Filtering	1. Verify that the **DoS Attacks** filter detects events in your environment that match the expected behavior. 2. Please make sure the following trend DoS Attacks Trend is enabled and deployed before running the weekly report on this use case.
Domain Policy Changes	This use case provides overview of domain policy changes.	AU-1	Operating Systems events (Windows)	

Dynamic Host Configuration Protocol (DHCP) Server	The Dynamic Host Configuration Protocol (DHCP) Server use case provides information about DHCP servers and IP leases in the network.	IA-3	DHCP Servers	Deploy the rules on this use case to the real-time rules group, and enable case and notification actions if appropriate for your organization.
E-Authentication Overview	This use case provides overview of E-Authentication assets on the organization.	CM-8|PM-5	All	Categorize assets or zones into the following groups: All Asset Categories/ ArcSight Solutions/ Compliance Insight Package/Regulation/ FISMA/ NIST 800-63/E-Authenticaiton
Email Activity	This use case provides information about email activity.	PL-4,SI-4,SI-8	Email Servers (Microsoft Exchange) Intrusion Detection Systems Intrusion Prevention Systems	Please make sure before deploying the rules and use the resources on this case to configure the following active lists: 1.Competitors :This list stores competitor email domains on lower case, for example if the user email format of your competitor is jsmith@example.com, then the email domain in this example is “example.com” (what goes after the @ in lowercase). 2. Important Emails: This list stores important emails of high-profile targets on the organization like C-lever executives which could be targeted by spear phishing attacks. Entries in this list should be in all lower case.
Event Distributions	This use case shows events distribution by various categorizations.	AU-2	All Devices	
FIPS-199 Assets Overview	This use case provides overview of assets in FIPS-199.	CM-5	SIEM(Arcsight)	Certain content does not display unless assets or zones are categorized. Categorize assets or zones into the following groups: Site Asset Categories/Compliance Requirement/FIPS-199

Failed Anti-Virus Signature Updates	This use case provides information about failed anti-virus signature updates on the organization.	SI-2	Anti-Virus	Verify that the Failed Anti-Virus Updates filter detects events in your environment that match the expected behavior
File Activity	This use case provides information about file activity on the organization, it's based on integrity checker tools and windows events.	SI-7	Integrity Tools	Verify that the File Creations, File Modifications, File Deletions filters detects events in your environment that match the expected behavior
Firewall Configuration Changes	This use case provides overview of firewall devices configuration changes.	CM-3	Firewalls	1. Verify that the Firewall Configuration Modifications filter detects events in your environment that match the expected behavior 2. Categorize all Firewall assets or zones in the below groups : /Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall
Firewall Traffic Overview	The Firewall Traffic Overview use case reports on a variety of firewall traffic controls, including blocked inbound and outbound traffic, and any open ports in your environment.	SC-7	Firewalls	Verify that the Firewall Accepts AND Firewall Deny filters detects events in your environment that match the expected behavior
Former Employee Account Activity	This use case provides information about any activity performed by users who are known to be terminated.	AC-4,PL-4,PS-4	Operating Systems (Windows)	1. Adding the organizational active directory Domains to Active Directory Domains Active List. 2. Verify that the Former Employee Account Detected filters detects events in your environment that match the expected behavior

Hacker Tools	This use case provides information about hacker tools detected on the organization.	SI-3	Proxy	Please make sure the rule : Hacker Tool Detected is enabled and deployed before running Hacker Tools Activity report
High Risk Events	This use case displays an overview of the events that require most attention.	IR-6	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Anti-Virus Physical Security Systems Wireless Applications Network Based Anomaly Detection	Verify that the High Priority Events filter detects events that require immediate attention.
Honeypot Activity	This use case provides overview about honeypot activity against the organization.	SC-26	Honeypot (modern honey network)	Verify that the Honeypot Interaction Activity filter detects events that require immediate attention.

Identity Management Policy Changes and Violations	This use case provides overview of identity management policy changes and violations.	IA-1	Identity Management	
Inactive User Accounts	The purpose of this use case is to identify user accounts that have not been active for a certain period of time, and to then identify activity from such stale accounts.	AC-2	Operating Systems Databases Applications Firewalls Virtual Private Networks (VPN) Identity Management Systems Policy Management Network Equipment Physical Security Systems	1. In the **Active Accounts** active list, set the appropriate TTL value for your organization. The TTL value specifies the timeframe by which an account is considered “stale” if no successful logins to the account have occurred. When a successful login to an account occurs, the account is placed on the **Active Accounts** active List. If, for example, the TTL value is 30 days, then if no successful login event to that account occurs in the next 30 days, the account expires from the **Active Accounts** active list and is placed on the Stale Accounts active list. When a login attempt (either successful or failed) is identified from an account on the Stale Accounts active list, a case is opened. 2. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. 3. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. User Logged in - Added to Active Accounts List Login Activity by a Stale Account Inactive User Account Detected Suspicious Activities by a Stale Account

Inbound Traffic	This use case provides information about inbound traffic.	AC-17	Firewall Proxy Intrusion Detection Systems Intrusion Prevention Systems	1. In the Insecure Processes active list, add any processes that your organization knows to be insecure. 2. In the Insecure Ports active lists, add the ports that your organization knows to be insecure. 3. Verify that the Inbound Events, Insecure Services filters detects events in your environment that match the expected behavior.
Incident Management	The Incident Management use case provides information about open cases which related to FISMA package.	IR-5	All	1. Please make sure the following trend Case History is enabled and deployed before running the following reports: Average Time to Resolution - By Case Severity, Average Time to Resolution - By Day, Average Time to Resolution - By User 2. Please make sure when deploying FISMA rules to enable cases actions when appropriate for your organization.

Information Disclosure Monitoring	This use case identifies and reports on all kinds of information leaks that may have occurred.	AU-13	Firewalls Intrusion Detection Systems Content Monitoring Systems	1. Verify that the Personal Information Leak and the Organizational Records Leak filters detects events in your environment that match the expected behavior. 2. Certain content does not display unless assets or zones are categorized. 3. Privileged Accounts Involved on Information Leaks report depends on the following active list Administrative Accounts please make sure to defines usernames that have administrative privileges in your environment. Entries should be lowercase only. 4. Former Employee Involved on Information Leaks report depends on the following active list **Former Employees** please refer to **Former Employee** Account Activity use case how to define this active list. 5. New Hire Involved on Information Leaks report depends on the following active list **New Hire Account**Please refer to New Hire Activity use case how to define this active list. 4. Inactive Employee Involved on Information Leaks report depends on the following active list **Stale Accounts** Please refer to Inactive User Accounts use case how to define this active list.
Information Interception	This use case identifies and reports on possible kinds of information interception events incidents such as spoofing attempts, man-in-the-middle attacks or instant messaging.	SC-23	Firewalls Intrusion Detection Systems Virtual Private Networks (VPN) Network Based Anomaly Detection	1. Verify that the Information Interception filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Information Interception rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

Information System Audit Tool Usage	This use case shows logins to information security audit tools.	AU-5,AU-9	SIEM (ArcSight Internal Events)	1. Verify that the Information System Audit Tool Login filter detects logins to all information security audit tools. 2. FISMA Report not Accessed more than Policy Standard Fires when an entry expires out of the referenced active list on this use case, signifying that the FISMA report didn't accessed within the prescribed time. Time limit is defined by the TTL in the active list (default 30 days). Before deploying this rule make sure “FISMA Report Accessed" rule is enabled and deployed.

Information System Failures	This use case provides overview of information system failures.	CA-7	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Antivirus Physical Security Systems Wireless Applications Network Based Anomaly Detection	1. Verify that the Information System Failures filter detects events in your environment that match the expected behavior. 2. Certain content does not display unless assets or zones are categorized.

Insecure Communications	This use case provides information about unencrypted and thus insecure communications inside the network.	SC-8	Firewall Proxy Intrusion Detection Systems Intrusion Prevention Systems	1. In the Insecure Processes active list, add any processes that your organization knows to be insecure. 2. In the Insecure Ports active lists, add the ports that your organization knows to be insecure. 3. Verify that the Inbound Events, Outbound Events, Insecure Services filters detects events in your environment that match the expected behavior. 4. Certain content does not display unless assets or zones are categorized.
Insecure Cryptographic Storages	This use case provides overview of insecure cryptographic storages on the organization.	SC-28, RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case

Insider Threat	This use case provides information about insider threats.	PM-12	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Antivirus Physical Security Systems Wireless Applications Network Based Anomaly Detection	1. Certain content does not display unless assets or zones are categorized. 2. Verify that the Insider Threat filters detects events in your environment that match the expected behavior.
Installed Windows Services	This use case provides information about installed windows services.	SI-4	Operating Systems (Windows)	Verify that the **Installed Windows Services** filter detects events in your environment that match the expected behavior.

Internet Activity	This use case provides overview of internet activity on the organization.	AC-14,PL-4	Firewall Proxy	1. Verify that the Outbound Internet Activity filter detects events in your environment that match the expected behavior 2. In the Internet Ports active lists, add the ports that your organization use for Internet communication. 3. Certain content depends on the following active lists Former Employee **Monitored Accounts** **New Hire Accounts** **Administrative Accounts** Please make sure those active lists are configured as expected.

Logging Devices	This use case provides overview of different products that are logging to ArcSight ESM.	AU-6	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Vulnerability Assessments Identity Management Policy Management Network Equipment Content Security Web Filtering Antivirus Physical Security Systems Wireless Applications Network Based Anomaly Detection	
Login Activity to Classified and Critical Machines	This use case provides overview of login activity to classified and critical machines.	AC-3	Operating Systems	1. Categorize assets or zones as Top Secret, Secret, or Unclassified in the /Site Asset Categories/Business Impact Analysis/Classification group. 2. Categorize assets or zones in one of the following groups: /System Asset Categories/Criticality/High /System Asset Categories/Criticality/Very High

Maintenance Monitoring	This use case provides different resources for monitoring maintenance operations.	MA-2	Operating Systems Applications Databases Network Equipment Content Security Firewalls Applications Virtual Private Networks (VPN) Wireless	1. In the Maintenance Window filter, define the allowed maintenance window for your organization. The default maintenance windows are from 3:00 a.m. to 3:59 a.m. on Sundays, and 4:00 a.m. to 4:59 a.m. on Wednesday. You can change this filter to adjust the default settings as appropriate for your environment. The filter uses two variables: The **WeekDay** variable returns an integer value that is displayed on the ArcSight ESM Console as a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, or Friday. Because the WeekDay variable is an integer, you can specify a range of days such as (WeekDay >= Monday AND WeekDay <= Friday). The **HourOfDay** variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23. To define the Maintenance windows of Tuesday morning, 1:00 AM to 2:59 AM, and Friday morning, 5:00 AM to 5:59 AM, use the following filter expression: (WeekDay = Tuesday AND HourOfDay >= 1 AND HourOfDay < 3) OR (WeekDay = Friday AND HourOfDay = 5) If you build a resource that refers to this filter, use the NOT operator when referring to it to exclude events that occur in this time window. 2. Categorize assets or zones in one of the following groups: /System Asset Categories/Criticality/High /System Asset Categories/Criticality/Very High

Malware Activity	This use case provides information about malicious software activity on the organization.	SI-3	Anti-Virus	1. Categorize internal zones and assets as /Site Asset Categories/Address Spaces/Protected2. Verify that the following filters detect events in your environment that match the expected behavior for each filter: **Malware Activity** **Anti-Virus Clean or Quarantine Attempt** **Spyware Activity** **Trojan Activity** **Virus Activity** **Worm Activity** **Failed Virus Removal Attempt**
Meltdown and Spectre Vulnerabilities	This use case provides overview about Meltdown and Spectre vulnerabilities.	SC-39	Vulnerability Assessments	1. Verify that the following filter **Meltdown|Spectre Vulnerability Detected** detect events in your environment that match the expected. 2. Verify and Configure Meltdown and Spectre Signatures Active List when required to add more signatures which supported on your environment.
Mobile Code Detection	This use case provides information about mobile code detected.	SC-18	Vulnerability Assessments Intrusion Detections Intrusion Prevention	1. Verify and Configure Mobile Code Detection Signatures Active List when required to add more signatures

Monitored Accounts	This use case provides information about monitored accounts activity.	PS-3,PL-4,AU-13,AC-2	Operating Systems Applications Databases Network Equipment Content Security Firewalls Applications Virtual Private Networks (VPN) Wireless Intrusion Detection Systems Intrusion Prevention Systems	Make sure to add users that you want to monitor to Monitored Accounts Active list in lower case.

NIST 800-53 Impact Assets Overview	This use case provides an overview of NIST 800-53 high, low, moderate impact Systems.	CM-8	SIEM(Arcsight)	Configure all assets and zones into either the FIPS-199 or the NIST 800-53 categories: 1.Categorize assets or zones into one of the appropriate groups (High, Moderate, or Low) for each of the following Security Objectives: /Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality /Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality /Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality OR 2.Categorize assets or zones into the appropriate /ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53 group: [CIS2] High Impact [CIS3] Low Impact [CIS4] Moderate Impact
Network Device Configuration Changes	This use case provides overview of network devices configuration changes.	CM-3	IDS/IPS Firewalls Network Equipment's	Categorize all firewall, NIDS or network equipment assets or zones in the below groups: /Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall /Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS /Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network
Network IDS Configuration Changes	This use case provides overview of network IDS devices configuration changes.	CM-3	IDS/IPS	Categorize all NIDS assets or zones in the below groups: /Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS

New Hire Activity	This use case provides information about new hire accounts.	PL-4,PS3	Operating Systems	Verify that the filter: **New Hire Account** Detected detects events in your environment that match the expected behavior, by default it's based on windows account deleted event "4720", this filter requires additional configurations by adding the organizational active directory Domains to the "Active Directory Domains" Active List.
New Systems	This use case provides overview of new systems detected on the last period.	CM-6	All	Certain content does not display unless assets or zones are categorized.
Non Multi Factor Privileged Accounts Authentication	This use case provides information about non multi factor authentication of privileged accounts on the organization.	CM-6	Operating Systems IDM	1. Populate the Multi Factor Authentication Devices active list with all multi factor authentication devices on your organization. All the entries in this list must be in lowercase. 2. If you have non multi authentication devices that you want to exclude from this compliance scenario you can populate them with the Non Multi Factor Authentication Devices - Exception active list. 3. Populate the **Administrative Accounts** active list with the administrative accounts in your organization. All the entries in this list must be in lowercase.
Operating Systems Configuration Changes	This use case provides overview of operating system configuration changes.	CM-3	Operating Systems	
Overflow Vulnerabilities	This use case provides overview of overflow vulnerabilities (like buffer and heap overflow) on the organization.	RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case

PKI Certificate Validity	This use case provides insight into incidents where an invalid or expired Public Key Infrastructure (PKI) certificate was detected, or certificate database is tampered.	SC-17	Applications Virtual Private Networks (VPN) Intrusion Detection System Operating Systems	Review the Invalid or Expired Certificate filter to identify events associated with invalid or expired certificates, and then verify that the filter detects events in your environment that match the expected behavior. The Invalid or Expired Certificate report assumes that the certificate name is included in the Device Custom String1 event field. If it is not, modify as app.

Password Management	The purpose of this use case is to monitor password change events as well as to alert if a password has not been changed for a longer time than allowed by policy.	IA-5	Operating Systems Vulnerability Assessments	1. When a successful password change event is detected, the user name for whom the password was changed and the device that reported the event are placed on the Password Changes active list. An entry expiring from this active list indicates that the user has not changed the password on that device for longer than allowed by policy (as indicated by the TTL of the active list). In that case, Password not Changed for Longer than **Policy Standard** rule will detect the event and open a case. If the user changes his/her password within the time defined by the policy, a rule will detect this event and update the entry on the active list so it will not expire. The Password Management use case requires the following configuration for your environment. · In the Password Changes active, edit the TTL to reflect the maximum amount of time allowed between password changes according to your organization's policy. · Edit the Password Change Attempts filter to identify all password change attempts from devices on your system. By default, the filter detects only password change attempts on Microsoft Windows. Verify that the Password Change Attempts filter detects events in your environment that match the expected behavior. · Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. Password not Changed for Longer than Policy Standard Successful Password Change Minimum Password Age Changed to Less than Policy Standard Rule Fires when minimum password age changed to less than policy

				standard (default 60 days), you can change the default by editing rule condition : "passwordAgedtoInt < 60" from 60 to different value which reflects your policy standard. Minimum Password Length Changed to Less than Policy Standard Fires when minimum password length changed to Less than policy standard (default 15 days), you can change the default by editing rule condition : "minimumPasswordLength < 15" from 15 to different value which reflects your policy standard.
Password Spray Attacks	This use case provides information about password spray attacks.	IA-5	Operating Systems (Windows)	

Penetration Testing not Performed for Longer than Policy Standard	This use case provides overview when Penetration Testing not Performed for Longer than Policy Standard.	CA-8	Vulnerability Assessments	When a vulnerability scan event is detected on specific asset the scan are placed on the Vulnerability Scans active list. An entry expiring from this active list indicates that the there was no vulnerability scan for this asset for longer than allowed by policy (as indicated by the TTL of the active list). In that case, vulnerability scan not conducted for Longer than Policy Standard a rule will detect the event and open a case. If a vulnerability scan on specific asset conducted on time defined by the policy, a rule will detect this event and update the entry on the active list so it will not expire. This use case requires the following configuration for your environment. In the Vulnerability Scanned Assets active list, edit the TTL to reflect the maximum amount of time allowed to conduct vulnerability scan. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. 1. Vulnerability Scans 2. Penetration Testing not Performed for Longer than Policy Standard

Personal identifiable information monitoring	This use case provides different resources for monitoring personal identifiable information assets.	PA-3,AU-13	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Vulnerability Assessments	Certain content does not display unless assets or zones are categorized: Categorize all assets or zones in one or more categories in the /ArcSight Solutions/Compliance Insight Package/Network Domains group

Physical Access	This use case detects violations and reports on events related to physical security devices such as badge readers. Specifically, it detects after hour building access by contractors and local Logon from badged out employees.	PE-6	Physical Security Systems	1. Populate the Badges to Accounts active list with the badge ID, primary computer account for the badge holder, and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the words “Contractor” “Visitor” (case insensitive) in the employee type field. 2. Modify the After Hours filter to specify the appropriate after-business-hours window for your organization. 3. Verify the following: Physical Access Events filter correctly identifies events from Physical Security Systems Building Access filter correctly identifies building access events Successful Badge In filter correctly identifies events that are logged when an employee enters the facility Badge Out filter correctly identifies building leave events Successful Building Access Granting filter correctly identifies building access granting events. 4. Deploy the following rules to the real-time rules group, and enable case and notification actions if appropriate for your organization. • After Hours Building Access by Contractors • Badged Out Employee • Failed Access by the Same User to Multiple Buildings • Failed Building Access • Local Logon from Badged Out Employee • Potential Badge Cloned • Potential Piggybacking Attack • Badged Out Employee • Successful Badge In

				• Successful Badge Out
Policy Violations	This use case provides information about policy violations.	PL-1	Intrusion Detection Systems Firewalls Operating Systems Assessment Tools Applications Security Information Managers Identity Management Virtual Private Networks (VPN) Policy Management	1. Certain content does not display unless assets or zones are categorized: Categorize all assets or zones in one or more categories in the /ArcSight Solutions/Compliance Insight Package/Network Domains group 2. Verify that the Policy Violations and Policy Breach filters detects events in your environment that match the expected behavior.
Possible Bitcoin Mining Activity	This use case provides information about possible bitcoin mining activity on your organization.	AC-23	Vulnerability Assessments (Nessus)	Verify that the filters Possible Bitcoin Mining Activity detects events in your environment that match the expected behavior, by default it's based on nessus plugin "56195" , This filter can be configured to support additional devices on your environment,
Ransomware Activity	This use case provides resources which helps with detecting ransomware activity on the organization.	SI-7	Operating Systems (Windows) Integrity Tools	The Rule : Potential Ransomware Activity on Critical Windows Machine Fires by default when there are 100 file changes (Multiple Files) from the same user and process on windows machine on 1 minute (Short Period of Time) This rule is based on windows event "4663". You can edit the aggregation tab to change the thresholds to different values which reflects your environment.

Reconnaissance Activities	This use case provides overview of recon activity.	IR-6,PM-12	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	1. Verify that the filters: Attacks with Geo Information Internal Recon Activity Reconnaissance - Geo Information Detect events in your environment that match the expected behavior 2. Certain content does not display unless assets or zones are categorized: Categorize all assets or zones in one or more categories in the /ArcSight Solutions/Compliance Insight Package/Network Domains group
Redirection Attacks	This use case provides information about redirection attacks.	SC-23	Firewalls Intrusion Detection Systems Virtual Private Networks (VPN) Network Based Anomaly Detection	1. Verify that the Information Redirection Attacks filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Redirection Attacks rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.
Remote Access Monitoring	This use case provides overview of remote accesses.	AC-17	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications VPN	Certain content does not display unless assets or zones are categorized under Solutions/Compliance Insight Package/Network Domains/Remote group.

Removable Media Activity	This use case provides information about removable media activity.	AC-20	Operating Systems (Windows)	1. Verify that the Removable Media Detected filter detects events in your environment that match the expected behavior. 2. Categorize assets or zones in one of the following groups: /System Asset Categories/Criticality/High /System Asset Categories/Criticality/Very High
Removal of Access Rights	This use case provides information about all activities when an access right of a user is removed.	AC-2,CM-5	Operating Systems	1. Verify that the Removal of Access Rights filter detects events in your environment that match the expected behavior. 2. Certain content does not display unless assets or zones are categorized: Categorize all assets or zones in one or more categories in the /ArcSight Solutions/Compliance Insight Package/Network Domains group
Replay Attacks	This use case identify replay attacks based on Microsoft 4649 event.	IA-2	Operating Systems (Windows)	

Resource Exhaustion	This use case provides overview of resource exhaustion on the organization.	AU-4	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Vulnerability Assessments Operating	Verify that the following filters detects events in your environment that match the expected behavior: Resource Exhaustion Security Log is Full
SQL Injection Vulnerabilities	This use case provides overview of sql injection vulnerabilities on the organization.	RA-5,SI-10	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
SSH Vulnerabilities	This use case provides overview about SSH vulnerabilities.	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
SSL and TLS Vulnerabilities	This use case provides overview about SSL and TLS vulnerabilities.	SC-13,RA-5	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
Security Application Stopped or Paused	This use case provides overview of security application stopped or paused (it focuses on Anti-Virus products).	SI-2	Operating Systems	1. Verify that the filters Anti-Virus Service Stopped or Paused and Anti-Virus Service Stopped or Paused in Windows detect events in your environment that match the expected behavior.
Security Patches	This Use Case provides information about missing security patches.	RA-5	Vulnerability Assessments	

Separation of Duties	This use case contains different resources which help to identify if separation of duties is not implemented on the organization.	AC-5,AC-9	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Operating Systems VPN	1. Categorize assets or zones on the following group: /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domain/ 2. The active list Test and Custom Accounts stores names of development, test, custom application or user accounts names make sure to Populate this active list with additional custom accounts that should be disabled in a production environment. 3. Verify that filters: Attacker is Custom Account Target is Custom Account Communications between Development and Operations Communications between Test and Operations Communications between Development and Test Detect events in your environment that match the expected behavior, by default this filter is based on windows events. This filter can be configured to support additional devices on your environment.

Session Termination	This use case provides overview about RDP sessions which not terminated for longer than policy standard.	AC-12	Operating Systems(Window)	1. Verify that filters : RDP Session Initiated RDP Session Terminated Detect events in your environment that match the expected behavior. 2. Configure this active list RDP Sessions TTL to specify how long should be the RDP session on your organization (default 1 day) 3. Before running the report RDP Session is not Terminated for Longer than Policy Standard please make sure the rules on this case are enabled and deployed.
Shell Code Attacks	This use case provides information about shell code attacks.	SI-3	IDS/IPS	1. Verify that the following filter Shell Code Execution Detected detects events in your environment that match the expected behavior. 2. Deploy the Shell Code Execution Detected rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

Shutdown of Machines	The Shutdown of Machines use case identifies when machines are shut down in your environment.	CP-2	Operating Systems	1. Categorize assets or zones in one of the following groups: /System Asset Categories/Criticality/High /System Asset Categories/Criticality/Very High /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domain/ 2. Verify that the following filters detects events in your environment that match the expected behavior. System Shutdown System Startup 3. Make sure the Shutdown of Critical Machines trend is enabled. 4. Shutdown of Highly Critical Machine rule fires when a shutdown of highly critical machine detected the event will be added as entry to the active list Critical Machines Shutdown Assets Startup of Highly Critical Machine rule fires when a startup of highly critical machine detected and relevant entry will be removed from the active list Critical Machines Shutdown Assets Shutdown Machine not Started more than Policy Standard rule Fires when an entry expires out of the Critical Machines Shutdown Assets active list (TTL in this active list is 1 hour), signifying that the shutdown machine didn't start within the prescribed time, update the TTL value on Critical Machines Shutdown Assets to satisfy your shutdown/startup policy of critical assets.
Software Changes	This use case provides information about software changes.	SI-7	Applications	Categorize zones and assets under /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domain

Software Inventory	The Software Inventory use case provides information about the software products detected in your environment.	CM-8,SI-7	Vulnerability Scanners (Nessus, eEye Retina) Integrity Tools	1. For Nessus connector, the Custom Nessus PluginID Service Map active list provides the list of services reported by a Nessus scanner. To report on additional custom services, add these custom services to the Custom Nessus PluginID Service Map active list. 2. Make sure the Software Detected trend is enabled. 3. If using a scanner other than Nessus or eEye Retina, configure the following filter to capture the appropriate events for your scanner: Software Detected, After configuration, verify that the Software Detected filter detects events in your environment that match the expected behavior for the filter.
Special privileges assigned to new logon	This use case provides overview of special privileges assigned to new logon.	AC-6	Operating Systems (Windows)	Verify that the filters Special privileges assigned to new log on detect events in your environment that match the expected behavior, by default this filter is based on windows events. This filter can be configured to support additional devices on your environment.

Third Party Activity	This use case provides overview of activity (like login, communication etc...) which involved third party asset.	AC-20,CA-3,RA-5,AC-5	Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications Vulnerability Assessments Operating Systems VPN	Model the third-party assets or zones in your environment and categorize them in /ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party.
Traffic Anomaly	This use case provides information about the traffic anomaly.	SC-8	Firewalls Intrusion Detection Systems Virtual Private Networks (VPN) Network Based Anomaly Detection	1. Verify that the Traffic Anomaly filter detects events in your environment that match the expected behavior. 2. Deploy the Possible Traffic Anomaly rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

Traffic Between Classification Levels	This use case shows which assets are communicating across different classification levels.	AC-4	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Proxy Wireless	1. Categorize assets or zones as Top Secret, Secret, or Unclassified in the /Site Asset Categories/Business Impact Analysis/Classification group. 2. Verify that the following filters detect events in your environment that match the expected behavior for each filter: Traffic from Higher to Lower Classification Level Traffic from Lower to Higher Classification Level 3. Deploy the following rules: High to Low Classified Traffic Information Leak Communication between Non Classified Machines and Classified Machines Domains to the real-time rules group, and enable case and notification actions if appropriate for your organization.
Traffic Between External and Internal Assets	This use case provides information about traffic that is flowing between internal and external assets.	CA-3	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Proxy Wireless	1. Categorize internal zones and assets as /Site Asset Categories/Address Spaces/Protected. 2. Verify the filters: **External to Internal Traffic** **Internal to External Traffic** Detect events in your environment that match the expected behavior.

Traffic Between Network Domains	This use case provides information about traffic that is flowing between various network domains.	AC-4	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Proxy Wireless	Categorize relevant assets or zones in the: ArcSight Solutions/Compliance Insight Package/Network Domains group
Traffic Between Network Zones	This use case provides information about the traffic flowing between various network zones.	AC-4	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Proxy Wireless	Verify the filters: **Traffic Between Network Zones** Detect events in your environment that match the expected behavior.
Traffic with Dark Address Space	This use case provides information about traffic with dark address space.	AC-4	Routers Intrusion Detection Systems Intrusion Prevention Systems Firewalls Network Equipment	1. Categorize relevant assets or zones in the /Site Asset Categories/Address Spaces/Dark group. 2. Verify the filters: **Traffic from Dark Address Space** **Traffic to Dark Address Space** Detect events in your environment that match the expected behavior.

Unauthorized Access to High Impact Systems	This use case provides overview of unauthorized access to high impact systems.	AC-3	Operating Systems	1. Update this active list Users Authorized to Access High Impact Systems to stores the usernames of the individuals who are authorized to access high impact systems. All the entries in this list must be in lowercase. 2.Categorize High Impact System zones and assets as /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST800-53/High-impact 3. Before running the report of this case make sure the following rule is enabled and deployed Unauthorized Access to High Impact Systems.
User Activity	The User Activity use case provides information about all successful and failed actions, such as scheduling tasks, logins, or account modifications performed by users in your environment.	AU-12,PL-4	Network Equipment Intrusion Detection Systems Intrusion Prevention Systems Firewalls Network Based Anomaly Detection Content Security Web Filtering	1. In the Administrative Accounts active list, define usernames that have administrative privileges in your environment. Entries should be lowercase only. 2. In the Internet Ports active lists, add the ports that your organization use for Internet communication.
User Groups Activity	This use case provides information about user groups.	AC-2	Operating Systems	

User Logged In From Two Countries	This use case shows login attempts with the same user name from two different countries.	SI-4,IA-2	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Identity Management Policy Management Network Equipment Content Security Web Filtering Wireless	1. By default, this use case works only for logins from public IP addresses. To detect login attempts from private IP addresses, associate all appropriate assets or zones with a location resource with a defined Country field. For example, if Asset1 and Asset2 are in two different countries, you should create two location resources, Location1 and Location2. Then, associate those location resources with the appropriate assets, for example Asset1 with Location1,Asset 2 with Location2 2. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. 3. Deploy the User Logged in from Two Countries rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

User Logged in from different IP Addresses	This use case provides information about single user names that have been used to login from different IP addresses.	IA-2	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Identity Management Policy Management Network Equipment Content Security Web Filtering Wireless Applications	1. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. 2. Deploy the User Logged in from different IP Addresses rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

User Logged in with Different User Names	This use case identifies attempts by the same user to log in using different user IDs.	IA-2	Intrusion Detection Systems Intrusion Prevention Systems Databases Operating Systems Firewalls Virtual Private Networks (VPN) Identity Management Policy Management Network Equipment Content Security Web Filtering Wireless Applications	1. Verify that the Successful Logins filter detects events in your environment that match the expected behavior. 2. Deploy the Same User Using Different User Names to Login rule to the real-time rules group, and enable case and notification actions if appropriate for your organization.

User Logins and Logouts	This use case provides information about the user logins and logouts.	IA-2,MP2	IDS/IPS Network Based Anomaly Detection Firewalls Network Equipment Content Security Web Filtering Antivirus Wireless Applications	1. In the Administrative Accounts active list, define usernames that have administrative privileges in your environment. Entries should be lowercase only. 2. By default, this use case processes only those events in which neither the source nor the destination users have administrative privileges. To change this default behavior to include events involving users with administrative privileges, edit the Non Administrative User. 3. Verify that the following filters detect the appropriate events: Login Attempts Logouts User Login Attempts Successful User Login Successful User Logout Unsuccessful User Login
VPN Access and Configuration Reporting	This use case provides insight into VPN access and configuration events.	AC-17	VPN	1. In the Administrative Accounts active list, define usernames that have administrative privileges in your environment. Entries should be lowercase only. 2. Verify that the filters on this use case detects events in your environment that match the expected behavior, The filters can be configured to support additional devices on your environment.
VPN Vulnerabilities	This use case provides overview about VPN vulnerabilities.	RA-5,SC-13	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case

Voice Over IP Attacks	This report provides overview of VOIP applications and attacks.	SC-19	Intrusion Detection Systems (Snort) Intrusion Prevention Systems Vulnerability Scanners	1. Categorize assets or zones in on the following groups: /ArcSight Solutions/Compliance Insight Package/Network Domain/VOIP 2.Verify that the following filters **Special privileges** assigned to new log on SIP 4XX Response VOIP Application Detected VOIP Attacks and Suspicious Activity VOIP Events VOIP Ghost Call Attack Detect events in your environment that match the expected behavior, by default this filter is based on windows events. This filter can be configured to support additional devices on your environment, 3. VOIP Applications Detection Signatures Active List contains a list of VOIP applications signatures, you can reconfigure it by adding more signatures relevant to your environment.
Voice over IP Vulnerabilities	This use case provides overview of VoIP vulnerabilities on the organization.	RA-5,SC-19	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case
Vulnerability Scanning	This use case provides information about vulnerabilities that might exist, and how they relate to defined assets.	RA-5	Vulnerability Assessments	1. Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly reports on this use case 2. Certain content does not display unless assets or zones are categorized.

Wireless Monitoring	This use case reports on wireless network activities based on events from Intrusion Detection Systems and Vulnerability Scanners.	AC-18	Vulnerability Assessments Wireless IDS—By default, the following wireless Intrusion Detection Systems: 1. AirMagnet 2. AirPatrol 3. AirDefense	1. If using a wireless IDS other than AirMagnet, AirDefense and AirPatrol, configure the following filters to capture the appropriate events for the IDS: Wireless Intrusion Detection Systems Rogue Station Detected Wireless Encryption Violation Wireless Malicious Traffic Detected Wireless Anomalous Traffic or Device Misconfiguration Detected 2. Before deploying the following rules: Wireless Security Protocol Vulnerability Detected Bluetooth Protocol Vulnerability Detected Make sure the Vulnerability Scanner Events Filter captures appropriate events on your organization. 3. Categorize assets or zones on the following group: /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domain/Wireless
Worm Activity	This use case provides overview of Worm activity on the organization.	SI-3	Antivirus Intrusion Detection Systems Intrusion Prevention Systems Network Based Anomaly Detection Firewalls Content Security Web Filtering	1. Verify that the following filter Worm Activity detect events in your environment that match the expected behavior

XSRF Vulnerabilities	This use case provides overview of XSRF vulnerabilities on the organization.	RA-5,SI-10	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case.
XSS Vulnerabilities	This use case provides overview of XSS vulnerabilities on the organization.	RA-5,SI-10	Vulnerability Assessments	Please make sure the following trend **Vulnerabilities** is enabled and deployed before running the weekly report on this use case

Appendix A: CIP for FISMA Resource Reference

This section lists all the resources of the FISMA compliance package .

Resource	Type	URI	Description
Account Creations , Deletions and Modifications	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows a live feed of events of account creations, deletions and modifications.
Privileged Account Changed	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows a real-time feed of events reflecting alteration of privileges. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Removal of Access Rights	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows a live feed of events reflecting the removal of a user's access privileges.
Login Activity from Non Classified Machines to Classified Machines	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Shows all the login activity from non classified machines to classified machines.
Successful Logins to Critical Machines	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Shows all successful logins to critical machines.
Traffic Between Network Domains	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This Active Channel shows all the traffic between network domains.
Traffic Between Zones	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the network traffic between zones, in case you need to limit this active channel to specific devices or events you can use the "Event Limit" filter.
Traffic to and from Classified Machines	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the network traffic going to or coming from machines which are categorized with the Site Asset Categories/Classification category.

Traffic to and from Dark Address Space	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the network traffic going to or coming from the dark address space.
Account Lockouts	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows account lockouts events.
Workstation Locked\Unlocked Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Shows events where a workstation locked\unlcoked.
VPN Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Looks for VPN configuration change events.
Wireless Anomalous Traffic or Device Misconfiguration	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This active channel shows all alerts when wireless anomalous traffic or device misconfiguration is detected.
Technical Compliance Check Failures	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This active channel looks for events which indicate that a technical compliance check failed, meaning that an either misconfigured system or system with severe vulnerability was found.
Information System Failures	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This active channel looks for information system failures.
Resource Exhaustion	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Looks for events that indicate resource exhaustion.
Security Log is Full	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Looks for windows events that indicate that the security log is full.

Audit Log Cleared	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Looks for events that indicate an audit log is cleared.
Information System Audit Tool Logins	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This active channel shows all the logins to the Information System Audit Tool - ArcSight.
All Information Leak Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This active channel shows real-time feed of events reflecting information leakage.
Organizational Information Leak Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This active channel shows real-time feed of events reflecting organizational information leakage.
Personal Information Leak Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This active channel shows real-time feed of events reflecting personal information leakage.
Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Looks for non ArcSight events that indicate configuration changes.
Database Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Looks for database configuration change events.
Firewall Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Looks for firewall configuration change events.
Network IDS Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	This active channel looks for NIDS configuration changes events.

Network Routing Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Looks for network routing configuration change events.
Operating Systems Configuration Changes	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Looks for operating systems configuration change events.
Critical Assets Resource Exhaustion	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This active channel shows critical systems resource exhaustion.
Critical Systems Startup and Shutdown	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This active channel shows critical systems startup and shutdown events .
Information System Failures on Critical Assets	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This active channel looks for information system failures on critical assets.
Default Vendor Account Used	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a real-time feed of events reflecting the use of vendor-provided default credentials. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Login Attempts	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a real-time feed of logout events.
Logouts	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a real-time feed of events where a logout attempt was made.

Replay Attacks	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	filter events identifying replay attacks based on Microsoft event ID 4649.
All Attacks and Suspicious Activity Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This active channel shows all attack and suspicious activity events.
High Priority Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This active channel shows high priority events which translate into high risk.
Internal Reconnaissance	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This active channel shows reconnaissance events originating internal to the corporation.
Physical Security	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows all physical access related activities.
Policy Violations	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Looks for policy violations in the past.
Vulnerability Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Looks for events that indicate the existence of vulnerabilities.
DoS Attacks	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This active channel shows events that are attributed to denial of service attacks.
Invalid or Expired Certificate Presented	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Shows a real-time feed of events which indicate that an invalid or expired certificate was detected.

Information Interception	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This active channel shows events that represent a possible interception of data over a 2 hour continuously sliding window.
Anti-Virus Stopped or Paused Events	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Looks for events indicating that anti-virus/security application stopped or paused on the last hour. for list of the default security applications supported refer to the Filter tab on the following filters : Anti-Virus Service Stopped or Paused Anti-Virus Service Stopped or Paused in Windows
Failed Anti-Virus Signature Updates	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Looks for failed anti-virus signatures updates on the last hour.
Failed Virus Removal Attempt	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Looks for events when an attempt to remove or quarantine a virus on a host failed.
Active Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores user names who have successfully logged in within the last 30 days.
Active Directory Domains	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains all the AD domains. This list is used on different scenarios like detecting when user account is deleted, enabled, disabled or special privileged assigned to new logon.
Administrative Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list should be populated with the usernames that have administrative privileges in your domain.Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure. This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".
Allowed Ports	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.

Audit Log Cleared	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list should be populated only by the rule Audit Log Cleared. It logs every time an audit log is cleared.
Badged In	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This list contains information about employees who are badged in.
Badged Out	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains the computer accounts of badged out employees.
Badges to Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This list contains the computer account and employee type for every physical device badge. Populate this active list with the badge ID, primary computer account for the badgeholder (in case its a visitor use the visitor user name), and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the word "Contractor" ,"Visitor" (case insensitive) in the employee type field.
Common Platform Enumeration	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains a list of Common Platform Enumeration strings based on MITRE CPE dictionary. You may need to put in product names reported by your scanner that do not match their dictionary names.
Competitors	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This list stores competitor email domains on lower case, for example if the user email format of your competitor is jsmith@example.com then the email domain in this example is example.com (what after the @ in lowercase).
Compliance Risk Score	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list maintains the compliance risk score for each regulation section. The compliance risk score is calculated based on the triggered rules in the solution package. You can manually change the score as required. This change will be reflected in the Compliance Risk Score dashboard.
Critical Machines Shutdown Assets	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores all the critical assets that shutdown and not restarted for the last x days. The default is 60 days. Do not manually update this active list.
Custom Nessus PluginID Service Map	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list provides the mappings from Nessus Plugin IDs to service names.

DMZ Assets	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This List should contains DMZ assets on the organization like DNS,WEB,SMTP servers. it contains 2 fields : IPAddress and AssetType where the hostname is the hostname of the asset and the AssetType is the type of the asset on lower case (by default supported 3 types dns,web,smtp). for example if your web server ip is x.y.z.w you should add it as IPAddress=x.y.z.w ,AssetType=web
Default Vendor Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.
Disallowed Ports	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains all disallowed destination ports. This active list should be populated according to your site policy.
Former Employees	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.
Important Emails	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This list stores important emails of high-profile targets on the organization like C-lever executives which could be targeted by spear phishing attacks. entries in this list should be in all lower case.
Insecure Ports	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list includes ports related to unencrypted and thus insecure communication services.
Insecure Processes	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list includes the names of processes that provide unencrypted and thus insecure communications.
Internal Systems with Insecure Services	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This list stores all internal systems with insecure services detected.
Internet Ports	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list includes ports that are used for Internet communication.
Meltdown and Spectre Signatures	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains Meltdown and Spectre vulnerabilities signatures.
Mobile Code Detection Signatures	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains a list of mobile code detection signatures.

Monitored Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list is used to maintain user accounts to be monitored, entries in this list should be in all lower case.
Monitored FISMA Reports	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list is updated when a monitored FISMA report is accessed. Before enabling and deploying those rules : 1. FISMA Report Accessed 2. FISMA Report not Accessed more than x days make sure to populate this active list with the reports that you want to monitor. for example if you want to monitor this report /All Reports/Arcsight/Solution/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins please add the following entires to the active list : Report : /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins
Multi Factor Authentication Devices	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores the multi factor authentication devices,All the entries in this list must be in lowercase.
New Hire Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains newly hired users and is automatically populated by the "New Hire Detected" rule. New users are retained for 7 days in the list.
Non Multi Factor Authentication Devices - Exception	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores non multi factor authentication devices which you want to exclude, All the entries in this list must be in lowercase.
Non Scanned Assets	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores all the assets that are not scanned by vulnerability scanners on the last x days (default 60 days) . Do not manually update this active list, its entries are populated automatically when an entry of active list "Vulnerability Scanned Assets" is expired, and removed when an asset on the list is scanned.
Password Changes	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active is updated with the user and product information when a successful password change occurs.
RDP Sessions	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list is updated with session information when a successful windows RDP connection/disconnection occurs.

Stale Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list is used to maintain user names that have not appeared in login events for the time specified by the Active Accounts active list TTL value.
Suspicious Activities by New Hires	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores events that were identified as attacks by new hires. The original event name is stored in the deviceCustomString1 field. By default, these events are stored for 60 days.
Test and Custom Accounts	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores names of development, test, or custom application or user accounts. Populate this active list with additional custom accounts that should be disabled in a production environment. All the entries in this list must be in lowercase.
Unsecured Password Signatures	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains unsecured password signatures.
Users Authorized to Access High Impact Systems	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores the usernames of the individuals who are authorized to access high impact systems. All the entries in this list must be in lowercase.
VOIP Applications Detection Signatures	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list contains a list of voip applications signatures.
Vulnerabilities on Development Environment	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores all the vulnerabilities on development environment, the TTL of this active list should be equal to the vulnerability scan frequency on the organization, for example if vulnerability scan conducted one for every 2 weeks the TTL Days should be at least 14 (default TTL 60).
Vulnerability Scanned Assets	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores all the assets that scanned by vulnerability scanners on the last x days. The default is 60 days. Do not manually update this active list.
Vulnerability Scanners	ActiveList	/All Active Lists/ArcSight Solutions/FISMA/	This active list stores the status of all vulnerability scanners detected on the last x days. The default is 60 days. Do not manually update this active list.
Account Creations , Deletions and Modifications	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This dashboard displays the last account creation, deletion and modification events.

Account Management Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows information related to user account activity.
Enabled and Disabled Accounts Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This Dashboard provides overview of enabled and disabled accounts.
Former Employee Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows information related to activity by former employees.
Inactive User Accounts Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This dashboard provides overview of inactive user accounts.
Privileged Account Changes	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This dashboard provides overview of privileged account changes.
User Group Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows information related to user group activity.
Login Activity from Non Classified Machines to Classified Machines	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Provides overview of login activity from non classified machines to classified machines.
Traffic Between Network Domains	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This dashboard displays information about traffic between network domains.
Traffic Between Zones	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This dashboard displays information about traffic between network zones.
Traffic to and from Classified Machines	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Displays information about traffic between assets whose criticality is categorized differently.

Communications between Operations and Development Domains	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This dashboard provides communication overview between operations and development domains.
Account Lockouts	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Displays information about account lockouts.
Frequent Unsuccessful Logins	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This dashboard provides overview of frequent unsuccessful logins.
Disallowed Ports Communications	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Displays information around events to disallowed ports.
Potentially Problematic Remote Access	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Displays information about remote access by privileged users or non vpn remote connection
Attacks and Suspicious Activity to and from Wireless Resources	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This dashboard displays information about wireless devices involved in attacks and suspicious behavior.
Administrative Logins from Third Party Systems	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This dashboard displays information about administrative logins from third party systems.
Last State External Device Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Provides Real-time display of the last 20 external device activities and their status.
Technical Compliance Checking	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This dashboard displays different views of failed compliance checks.
Internal External Traffic	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This dashboard provides traffic overview between internal and external assets.

Information System Failures	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This dashboard displays information system failures.
Event Distribution	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This dashboard shows event distribution by various categorizations.
Resource Exhaustion	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	This dashboard provides overview of resource exhaustion on the organization.
Audit Log Cleared	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Displays Audit Log Cleared compliant status.
Administrative Actions	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This dashboard displays Administrative Actions information.
Failed Administrative Actions	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This dashboard displays Failed Administrative Actions information.
Information Leaks	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This dashboard displays information around information leakage.
Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about configuration changes.
Configuration Modifications by Network Domains	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks configuration modifications by network domain.

Database Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about database configuration changes.
Firewall Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about firewall configuration changes.
Network Devices Configuration Changes Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about network devices equipment (such as router, switch) configuration changes.
Network IDS Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about network IDS configuration changes.
Operating Systems Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays information about OS configuration changes.
Asset Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This dashboard displays asset creation, deletion, and modification activities.
Asset Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This dashboard shows data about assets currently present on ESM.
Assets with FIPS-199 Criticality Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This dashboard shows data about assets categorized with FIPS-199.
NIST 800-53 Categorized Assets by Impact	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This dashboard shows data about assets categorized with NIST 800-53 High/Moderate/Low Impact categorizations.

Operating System Assets Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This Dashboard provides overview of Operating System Assets.
Software Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This dashboard shows an overview of the software detected in your environment.
Critical Assets and Zones Details	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This Dashboard provides overview of critical assets and zones.
Up Down Status of Highly Critical Assets	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This Last State data monitor shows the state of highly critical assets and whether they are up or down.
Administrative Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows an overview of the administrative login and logouts activity on the organization.
Default Vendor Account Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the uses of default vendor accounts.
General User Login Attempts	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows an overview of user login attempts on the organization.
Non Multi Factor Administrative Authentication	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This dashboard provides overview of non multi factor administrative authentication.

Unsuccessful Administrative Logins	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows an overview of unsuccessful administrative logins activity on the organization.
Unsuccessful User Logins	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows an overview of unsuccessful user activity on the organization.
User Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows an overview of the user login and logouts activity on the organization.
Accesses Through AAA Server	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This dashboard provides overview of accesses/rejects through AAA Server.
DHCP Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This dashboard presents overview information about DHCP events.
Open Cases	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This dashboard displays information about open cases.
Attacks and Suspicious Activities - Investigation	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This dashboard displays an overview of information about attacks and suspicious activity events and used to investigate attacks using its drill down mechanism.
Attacks and Suspicious Activity Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This dashboard displays overview information about attacks and suspicious activity events.

Reconnaissance Sources	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This dashboard displays information about reconnaissance events and sources.
Risk - GeoView	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This dashboard provides a geographical view of potential threatening events.
Risk Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This dashboard displays high-level information around potential malicious events.
Unscheduled Changes	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This dashboard displays information about unscheduled changes.
Monitored Accounts Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This dashboard provides information about monitored accounts activity.
Physical Security Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Displays information around physical access.
Policy Violations	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Displays information about policy violations and violators.
Email Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This dashboard presents an overview of Email Activity in the enterprise.
Internet Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This dashboard provides overview of internet activity by different user groups.
New Hires Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows information related to activity by new hire employees.

Insider Threat	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This dashboard displays information about insider threats.
Internal Reconnaissance	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This dashboard displays information about internal reconnaissance events.
Last State Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides real-time compliance status of the last 20 vulnerabilities. Compliance Status is determined using the following : Agent-Severity =High or Very-High -> Violation Agent-Severity =Medium -> Possible Violation Agent-Severity =Low -> Compliant
Missing Security Patches	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Displays missing security patches.
Overflow Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of overflow vulnerability events.
SQL Injection Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This Dashboard provides overview of sql injection vulnerability events.
Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability events.
Vulnerability Scans	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability scanners and scans on the organization, the user can drill down from this dashboard to various query viewers which provides detailed information about the vulnerabilities which detected by those vulnerability scanners.
XSRF Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of XSRF vulnerability events.

XSS Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of XSS vulnerability events.
DoS Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This dashboard provides an overview of events associated with denial of service and availability attacks.
Attacks and Suspicious Activity to and from Third Party Resources	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This dashboard displays information about third party assets involved in attacks and suspicious behavior.
Blocked Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This dashboard shows information related to blocked traffic activity.
Insecure Services	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This dashboard displays information about unencrypted services.
Traffic Anomaly	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This dashboard displays information about traffic anomaly events.
Cryptographic Hash Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of cryptographic hash vulnerabilities.
Cryptographic Public Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of Cryptographic public key related Vulnerabilities.

Cryptographic Symmetric Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of cryptographic symmetric key related vulnerabilities.
Cryptographic Weak Protocol Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of cryptographic weak protocol vulnerabilities.
SSH Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of SSH Vulnerabilities.
SSL|TLS Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of SS/TLS Vulnerabilities.
VPN Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides an overview of VPN Vulnerabilities.
VOIP Attacks Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This dashboard provides overview of VOIP attacks on the organization.
VOIP Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Provides overview of voice over ip vulnerability events.
DNS Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This dashboard provides overview of DNS activity ,its based on ISC BIND events.

Information Interception	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This dashboard displays information about interception events.
Honeypot Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This dashboard provides overview of honeypot activity against the organization.
Insecure Cryptographic Storage	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	This dashboard provides overview of insecure cryptographic storage events on the organization.
Meltdown|Spectre Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	This dashboard provides overview of Meltdown and Spectre vulnerabilities.
Anti-Virus Stopped or Paused Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	This dashboard provides overview of anti-virus stopped or paused events.
Failed Anti-Virus Signature Updates	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	This dashboard provides overview of failed anti-virus signature updates.
Malware Activity Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This dashboard provides overview of general malware activity.
Malware Attackers Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This dashboard provides overview of malware attackers.
Malware Targets Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This dashboard provides overview of malware targets.

Worm Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This dashboard provides overview of worm activity on the organization.
Botnet Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This dashboard provides overview about Botnet activity on the organization. Before using this dashboard please make sure the following rule : Possible Botnet Activity is enabled and deployed
Phishing Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This dashboard displays information about phishing events.
Spam Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This dashboard displays information about spam events.
Development Domain Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This Dashboard provides overview of development domain traffic activity.
Development Login Activity	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This dashboard provides overview of the login activity on the development domain.
Compliance Risk Score	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard displays information about the compliance risk score for each regulation section.
NIST-AC Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST AC regulation section.
NIST-AT Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST AT regulation section.
NIST-AU Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST AU regulation section.
NIST-CA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST CA regulation section.

NIST-CM Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST CM regulation section.
NIST-CP Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST CP regulation section.
NIST-IA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST IA regulation section.
NIST-IP Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST IP regulation section.
NIST-IR Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST IR regulation section.
NIST-MA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST MA regulation section.
NIST-MP Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST MP regulation section.
NIST-PA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST PA regulation section.
NIST-PE Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST PE regulation section.
NIST-PL Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST PL regulation section.
NIST-PM Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST PM regulation section.
NIST-PS Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST PS regulation section.
NIST-RA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST RA regulation section.
NIST-SA Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST SA regulation section.
NIST-SC Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST SC regulation section.
NIST-SI Overview	Dashboard	/All Dashboards/ArcSight Solutions/FISMA/Overview/	This dashboard shows high-level information about NIST SI regulation section.
Distribution of Account Management Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This data monitor counts the types of different account management events.
Last 10 Disabled Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays last 10 disabled accounts.

Last 10 Enabled Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays last 10 enabled accounts.
Last 10 Former Employee Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 10 Logins by Stale User Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This data monitor shows login activity by stale user accounts.
Last 10 Privileged Account Changes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays events where authorization/access changes have been made to an administrative account.
Last 20 Information System Accounts Created	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 account creations.
Last 20 Information System Accounts Deleted	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 account deletions.
Last 20 Information System Accounts Modified	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 account modifications.
Last 20 User Group Created	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 user group creations.
Last 20 User Group Deleted	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 user group deletions.
Last 20 User Group Modified	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the last 20 user group modifications.
Suspicious Activity by Stale Users	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This data monitor shows the stale user suspicious activity count.

Top 10 Asset Network Domains with Account Creation Deletion and Modification	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays the Network Domains asset categories in which the most accounts have been created, modified or deleted.
Top 10 Domains with Disabled Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays top 10 domains with disabled accounts.
Top 10 Privileged Account Changes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Displays top changed administrative accounts.
Users Changing Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This data monitor shown the users that added, deleted and modified accounts.
Last 10 Logins from Non Classified Machines to Classified Machines	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	This data monitor shows login activity from non classified machines to classified machines.
Top 10 Logins from Non Classified Machines to Classified Machines	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Displays top 10 users which login from non classified machines to classified machines.
Classification Level Traffic High to Low	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows a graph of network traffic which went from a higher-classified asset to a lower-classified one.
Classification Level Traffic Low to High	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows a graph of network traffic which went from a lower-classified asset to a higher-classified one.
Internal Inter-Domain Traffic by Attacker Domain	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This data monitor shows the internal inter-domain traffic by attacker domain.

Internal Inter-Domain Traffic by Target Domain	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This data monitor shows the internal inter-domain traffic by target domain.
Last 10 Internal Inter-Domain Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This data monitor displays the last 10 Internal Inter-Domain Traffic.
Top Internal Inter-Domain Communications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This data monitor shows the top attacker and target domain pairs with most traffic.
Traffic Between Zones	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This data monitor shows the target ports between zones.
Last 10 Communications between Operations and Development Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This data monitor displays the last 10 communications between operations and development domains.
Top 10 Communications between Operations and Development Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This data monitor shows the top 10 communications between operations and development domains.
Account Lockouts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Displays events when an account has been locked out.
Disallowed Ports by Policy	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Provides the distribution of disallowed ports by policies.
Last 20 Successful Non VPN Remote Access Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the last 20 successful non VPN remote access events.
Last Connections to Disallowed Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the last 10 connections to disallowed ports to or from the network.

Non VPN Remote Access Attempts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows a moving average of unsuccessful non VPN remote access attempts. It displays data for the last 24 hours and will generate a correlation event if the moving average is increased by 300%.
Privileged Access on a Remote Connection	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Displays an Event Graph anytime a connection is reported by a VPN device, where the user name belongs to a privileged account.
Top Disallowed Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Provides a list of the top 10 disallowed ports.
Top Internal Hosts to Disallowed Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Provides a list of the top 10 internal hosts that accessed disallowed ports.
Top Internal Providers of Disallowed Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Provides a list of the top 10 internal providers of disallowed ports.
Attacks and Suspicious Activity Events in the Wireless Network Domain - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Wireless Network Domain.
Last 20 Attacks and Suspicious Activity Events Targeting Wireless Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Wireless asset or zone.
Last 20 Attacks and Suspicious Activity Events from Wireless Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Wireless asset or zone.
Ports Used in Attacks and Suspicious Activity Events Targeting Wireless Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This data monitor shows the ports used in attack and suspicious activity events that targeted Wireless assets or zones. By default the data monitor shows data from the last 5 minutes.

Ports Used in Attacks and Suspicious Activity Events from Wireless Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This data monitor shows the ports used in attack and suspicious activity events that originated from Wireless assets or zones. By default the data monitor shows data from the last 5 minutes.
Last 10 Successful Administrative Logins from Third Party Systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Provides a list of the last 10 successful administrative logins from third party systems.
Last 10 Unsuccessful Administrative Logins from Third Party Systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Provides a list of the last 10 unsuccessful administrative logins from third party systems.
Last State External Device Overview	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Real-time display of the last 20 external device activity and their status.
Top 10 Hosts with Successful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Provides a list of the hosts with most successful administrative logins from third party systems.
Top 10 Hosts with Unsuccessful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Provides a list of the hosts with most unsuccessful administrative logins from third party systems.
Last 20 Failed Technical Compliance Checks	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This data monitor shows the last 20 events indicating failed technical compliance checks.
Last 20 Machines Failing Technical Compliance Checks	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This data monitor reports the last 20 machines that were reported to have failed technical compliance check.
Top 10 Failed Technical Compliance Checks	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This data monitor shows the top ten events indicating failed technical compliance checks.

Top 10 Machines Failing Technical Compliance Checks	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This data monitor shows the top 10 machines with failed compliance checks.
Last 10 External to Internal Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This data monitor shows the last 10 external to internal traffic.
Last 10 Internal to External Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This data monitor shows the last 10 internal to external traffic.
Top 10 External to Internal Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This data monitor shows the top 10 external to internal traffic traffic.
Top 10 Internal to External Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This data monitor shows the top 10 internal to external traffic.
Last 10 Information System Failures Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This data monitor shows the last 10 information system failures events.
Top 10 Information System Failures Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This data monitor shows the top 10 information system failures assets.
Event Distribution by Category Object	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This data monitor shows the distribution of category object across all events.
Event Distribution by Category Outcome	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This data monitor shows the distribution of category outcome across all events.

Event Distribution by Device Group	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This data monitor shows the distribution of device group across all events.
Last 10 Resource Exhaustion Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Track the last 10 resource exhaustion events.
Last 10 Security Log is Full Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Track the last 10 security log is full events.
Top 10 Machines with Resource Exhaustion Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Tracks the top 10 machines with resource exhaustion events
Top 10 Machines with Security Log is Full Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Tracks the top 10 machines with security log is full events.
Audit Log Cleared Status	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Reports violation suspected status when an audit log cleared event is present.
Last 20 Audit Log Cleared Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Reports the last 20 audit log cleared events.
Administrative Actions by Device Moving Average	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows a moving average of administrative actions per device. Administrative accounts are defined by the filter Administrative User.
Administrative Actions by Username Moving Average	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows a moving average of administrative actions per username. Administrative accounts are defined by the filter Administrative User.

Failed Administrative Actions by Device Moving Average	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows a moving average of failed administrative actions per device. Administrative accounts are defined by the filter Administrative User.
Failed Administrative Actions by Username Moving Average	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows a moving average of failed administrative actions per username. Administrative accounts are defined by the filter Administrative User.
Last 20 Failed Administrative Action Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows the last 20 failed administrative actions. Administrative accounts are defined by the filter Administrative Users.
Outcome of Administrative Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows a moving average of the outcome of administrative actions.
Top 10 Administrative Users by Performed Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows the top 10 administrative users appearing in events in the last hour. Administrative accounts are defined by the filter Administrative User.
Top 10 Administrative Users with Failed Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows the top 10 administrative users with failed actions in the last hour. Administrative accounts are defined by the filter Administrative User.
Top 10 Devices with Administrative Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows the top 10 device products with actions by administrative users in the last hour. Administrative accounts are defined by the filter Administrative User.
Top 10 Devices with Failed Administrative Actions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This datamonitor shows the top 10 devices products with failed actions by administrative users in the last hour. Administrative accounts are defined by the filter Administrative User.
Organizational Records Leak	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This data monitor displays a graph with events which pertain to information leaks of organizational records.
Personal Information Leak	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This data monitor shows communications pertaining to personal information leaks.

Last 10 Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent system configuration modifications.
Last 10 Database Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent database configuration modifications.
Last 10 Firewall Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent firewall configuration modifications.
Last 10 Network Devices Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent network devices configuration modifications.
Last 10 Network IDSs Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent NIDSs configuration modifications.
Last 10 Network Routing Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent network routing configuration modifications.
Last 10 Operating Systems Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the most recent OS configuration modifications.
Top 10 Configuration Modifications Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the top 10 system configuration modifications.
Top 10 Database Configuration Modifications Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the top 10 database configuration modifications.

Top 10 Devices with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the assets that have their configurations changed frequently.
Top 10 Firewall Configuration Modifications Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the top 10 firewall configuration modifications.
Top 10 Firewalls with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the Firewalls that have their configurations changed frequently.
Top 10 Network Devices with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the network devices that have their configurations changed frequently
Top 10 Network IDS Configuration Modifications Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the top 10 network IDS configuration modifications.
Top 10 Network IDS with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the network IDSthat have their configurations changed frequently.
Top 10 Network Routings with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the network routings equipment that have their configurations changed frequently.
Top 10 Operating Systems Configuration Modifications Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks the top 10 OS configuration modifications.
Top 10 Operating Systems with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Provides a list of the operating systems that have their configurations changed frequently.

Top Configuration Modifications by Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks configuration modifications by network domain.
Last 10 Asset Creations	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This data monitor provides a list of the last ten assets created.
Last 10 Asset Deletions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This data monitor provides a list of the last ten assets deleted.
Last 10 Asset Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This data monitor provides a list of the last 10 asset modifications done to assets.
Last 10 Shutdowns of Highly Critical Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This data monitor displays the last 10 Shutdowns of Highly Critical Assets .
Top 10 Shutdowns of Highly Critical Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This data monitor shows the 10 highly critical assets with top shutdowns .
Up Down Status of Highly Critical Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This Last State data monitor shows the state of highly critical assets and whether they are up or down.
Last 10 Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.
Last 10 Successful Administrative Logouts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 10 administrative logouts across your assets categorized in Network Domains.

Last 10 Successful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 10 successful logins by non-administrative users across your assets.
Last 10 Successful User Logouts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 10 successful non-administrative user logouts across your assets.
Last 20 Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.
Last 20 Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the last 20 unsuccessful non-administrative user logins across your assets categorized in Network Domains.
Last 20 User Login Attempts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows in real-time the last 20 login attempts for non-administrative users across your assets.
Last Default Vendor Account Credentials Observed	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Displays login events where user has attempted to login to a system with vendor-supplied default User ID.
Top 10 Administrative Users with Successful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the administrative attacker and target user name pairswith most successful logins.

Top 10 Administrative Users with Unsuccessful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the administrative attacker and target user name pairs with most failedlogins.
Top 10 Hosts with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the hosts with most successful administrative logins.
Top 10 Hosts with Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a list of the hosts with most unsuccessful administrative logins.
Top 10 Hosts with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides an ordered list of hosts that most frequently have login failures for non-administrative users.
Top 10 Network Domains with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides an ordered list of the Network Domains with most successful administrative logins.
Top 10 Network Domains with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides an ordered list of the Network Domains that most frequently have non-administrative user login failures.
Top 10 Users with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides an ordered list of non-administrative users who most frequently have failed logins.

Top Default Vendor Accounts Observed	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Displays top vendor-supplied default account observed.
Top Targets with Default Vendor Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Displays login events where user has attempted to login to a system with vendor-supplied default account.
Top User Login Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top 20 non-administrative users attempting to login to a system.
Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Reports on a moving average of the number of unsuccessful user logins.
User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Reports on a moving average of the number of user logins.
Event Count by DHCP server in Last Hour	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This data monitor shows the top DHCP servers with most events in the last hour.
Events by Process in Last Hour	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This data monitor shows the top DHCP servers with the most events in the last hours.

Last 10 Accepted Accesses Through AAA Server	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	Provides a list of the last 10 accepted accesses through AAA Server.
Last 10 Rejected Accesses Through AAA Server	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	Provides a list of the last 10 rejected accesses through AAA Server.
Last 20 DHCP Critical Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This data monitor shows the last 20 DHCP critical events.
Top 10 Hosts with most Rejected Accesses	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	Provides an ordered list of hosts that most frequently have rejected accesses.
Top 10 Rejected Users	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	Provides an ordered list of the top rejected users through AAA server.
Top Clients with Most New or Renewed Leases in Last 2 Hours	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This data monitor shows the top DHCP clients with most requests in the last hour.
All Attacks - GeoView	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows all the attack events on a map.
Attacks and Suspicious Activity Event Names - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows connections between source and destination machines and event names as they appear in attack and suspicious activity events.

Attacks and Suspicious Activity Event Ports - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events.
Attacks and Suspicious Activity per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	Shows a moving average of attacks. It displays data for the last hour and will generate a correlation event if the moving average is increased by 300%.
Compromised Hosts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This Last State data monitor shows the last compromised hosts.
Last 10 High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor displays in real-time the last 10 high risk events.
Last 10 Reconnaissance Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor displays in real-time the last 10 reconnaissance events.
Last 20 Attacks and Suspicious Activity Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor displays the last 20 attack and suspicious activity events.
Ports Used in Attacks and Suspicious Activity Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows the ports used in attack and suspicious activity events. By default the data monitor shows data from the last 5 minutes.
Reconnaissance Only - GeoView	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows all reconnaissance events on a world map.
Top Hosts with High Risk Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	Provides an ordered list of the top hosts with high priority events.
Top Reconnaissance Attacker Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows the top reconnaissance attacker countries.

Top Reconnaissance Attacker Zones	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows the top reconnaissance attacker zones.
Top Reconnaissance Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This data monitor shows the top reconnaissance attackers.
System Shutdown or Restart at Unscheduled Time	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This data monitor shows events when a system shutdown or restart happens outside of the scheduled maintenance window.
Unscheduled Change of Service	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This data monitor shows events where a change of service was affected on a host outside of the scheduled maintenance window.
Last 10 Email Activity by Monitored Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This data monitor displays in real-time the last 10 email activity by monitored accounts.
Suspicious Activity by Monitored Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Shows the monitored account suspicious activity count. Suspicious activity is counted for 7 days (as long as the user is defined new, see New Hire Accounts active list).
Top Monitored Accounts with Unsuccessful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Provides an ordered list of the top monitored accounts with unsuccessful logins.
Building Access - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Used to show the hour of day that users are accessing buildings.
Contractor Access After Hours	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the top contractors accesses after hours.
Last 20 Building Access Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the last 20 physical access events.

Top Users Accessing Buildings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the top 10 users accessing buildings.
Top 10 Policy Violations	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 10 policy violation events.
Top 10 Policy Violators	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 10 policy violators.
Emails Sent	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This data monitor shows a moving average of the number of emails sent.
Internet Activity by Former Employee	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows Internet activity per reporting device per new hire over a day's period.
Internet Activity by Monitored Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows Internet activity per reporting device per new hire over a day's period.
Internet Activity by New Hires	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows Internet activity per reporting device per new hire over a day's period.
Internet Activity by Privileged Accounts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows Internet activity per reporting device per new hire over a day's period.
New Hires Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows the new hire user logins.
Suspicious Activity by New Hires	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows the new hires suspicious activity count. Suspicious activity is counted for 7 days (as long as the user is defined new, see New Hire Accounts active list).

Top Email Receivers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This data monitor shows the top email receivers based on the number of emails received.
Top Email Senders	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This data monitor shows the top email senders based on the number of emails sent.
Insider Threat per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	Shows a moving average of severe attacks originated from internal assets against internal assets. It displays data for the last hour and will generate a correlation event if the moving average is increased by 300%.
Internal Reconnaissance	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This Event Graph data monitor shows all internal reconnaissance activity.
Last 10 Internal Reconnaissance Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This data monitor displays in real-time the last 10 Internal Reconnaissance Events.
Top Insider Threat Sources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This data monitor shows the top insider threat sources.
Top Insider Threats Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This data monitor shows the top insider threat targets.
Top Internal Reconnaissance Sources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This data monitor shows the top internal reconnaissance sources identified by the rule in this section.
Top Internal Reconnaissance Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This data monitor shows the top internal reconnaissance targets.

Last 10 Security Patch Missing Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Displays in real-time the last 10 security patch missing events.
Last 20 Overflow Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides real-time display of the last 20 overflow vulnerabilities.
Last 20 SQL Injection Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides real-time real-time display of the last 20 SQL vulnerabilities.
Last 20 Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the last 20 vulnerabilities.
Last 20 Vulnerabilities with High CVSS	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the last 20 vulnerabilities with CVSS equal or higher than 8.
Last 20 XSRF Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides real-time display of the last 20 XSRF vulnerabilities.
Last 20 XSS Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides real-time display of the last 20 XSS vulnerabilities.
Last State Vulnerability Overview	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the last 20 vulnerabilities related to assets and their compliance status.
Top 10 Assets missing Security Patches	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with security patches missing.
Top 10 Assets with Critical Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with critical vulnerability events.
Top 10 Overflow Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with overflow vulnerability events.

Top 10 SQL Injection Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with sql injection vulnerability events.
Top 10 Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with vulnerability events.
Top 10 XSRF Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with XSRF vulnerability events.
Top 10 XSS Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows real-time display of the top 10 assets with XSS vulnerability events.
DoS Attacks Event Ports - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This data monitor shows connection between attacker and target machines and ports as they appear in denial of service attack events.
Last 20 DoS Attack Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This data monitor displays the last 20 denial of service attack events.
Top 10 DoS Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This data monitor shows the top 10 DoS Attackers.
Top 10 DoS Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This data monitor shows the top 10 DoS attacker countries.
Top 10 DoS Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This data monitor shows the top 10 DoS targets.

Attacks and Suspicious Activity Events in the Third Party Network Domain - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Third Party Network Domain.
Blocked Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor presenting blocked traffic in event graph chart .
Last 10 Blocked Traffic Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor shows the last 10 blocked traffic events.
Last 20 Attacks and Suspicious Activity Events Targeting Third Party Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor displays the last 20 attack and suspicious activity events where the traffic is destined for a Third Party asset or zone.
Last 20 Attacks and Suspicious Activity Events from Third Party Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor displays the last 20 attack and suspicious activity events where the traffic originated from a Third Party asset or zone.
Ports Used in Attacks and Suspicious Activity Events Targeting Third Party Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor shows the ports used in attack and suspicious activity events that targeted Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.
Ports Used in Attacks and Suspicious Activity Events from Third Party Resources	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor shows the ports used in attack and suspicious activity events that originated from Third Party assets or zones. By default the data monitor shows data from the last 5 minutes.
Top Blocked Traffic Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This data monitor displays a bar chart of the top attacker addresses of blocked traffic.

Insecure Services Communication by Address	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor shows a graph view of insecure traffic from a particular source address to a destination address.
Insecure Services Communication by Zone	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor shows a graph view of insecure traffic from a particular source zone to a destination zone.
Top Insecure Transmissions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor shows top 10 communications using inherently insecure services. Such services are listed in the referenced filter.
Top Insecure Transmissions Between Zones	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor shows top 10 communications, sorted by attacker and target zones, using inherently insecure services. Such services are listed in the referenced filter.
Top Traffic Anomaly Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor provides a list of the top 10 anomaly traffic per Attacker and Target Addresses addresses .
Traffic Anomaly	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor presenting traffic anomaly in event graph chart .
Traffic Anomaly by Protocol	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This data monitor provides the distribution of traffic anomaly by protocol.

Last 10 Cryptographic Hash Algorithm Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 cryptographic hash related vulnerabilities.
Last 10 Cryptographic Public Key Related Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 cryptographic public key related vulnerabilities.
Last 10 Cryptographic Symmetric Key Related Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 cryptographic symmetric key related vulnerabilities.
Last 10 Cryptographic Weak Protocol Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 cryptographic weak protocol related vulnerabilities.
Last 10 SSH Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 SSL/TLS vulnerabilities.
Last 10 SSL|TLS Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 SSL/TLS vulnerabilities.
Last 10 VPN Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the last 10 VPN vulnerabilities.
Top 10 Cryptographic Hash Algorithm Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with cryptographic hash algorithmrelated vulnerabilities.
Top 10 Cryptographic Public Key Related Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with cryptographic public key related vulnerabilities.

Top 10 Cryptographic Symmetric Key Related Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with cryptographic symmetric Key related vulnerabilities.
Top 10 Cryptographic Weak Protocol vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with cryptographic weak protocol-related vulnerabilities.
Top 10 SSH Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with SSL vulnerabilities.
Top 10 SSL|TLS Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with SSL vulnerabilities.
Top 10 VPN Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Provides real-time display of the top 10 assets with SSL vulnerabilities.
Last 10 VOIP Attack Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This data monitor displays the last 10 VOIP attack events.
Last 20 VOIP Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Provides real-time display of the last 20 voice over ip vulnerabilities.
Top 10 VOIP Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This data monitor shows the top 10 VOIP Attackers.
Top 10 VOIP Target Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This data monitor shows the top 10 VOIP targets assets.

Top 10 VOIP Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This data monitor shows the top 10 VOIP targets assets.
Top 10 VOIP Vulnerable Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Shows real-time display of the top 10 assets with voice over ip vulnerability events.
DNS Queries - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This data monitor shows connections between attacker machines and event names and queried domains.
Last 10 DNS Query Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This data monitor displays the last DNS query events.
Top 10 DNS Domains Queried	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This data monitor shows the top 10 DNS domains queried.
Top 10 DNS Originator IPs	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This data monitor shows the top 10 DNS queries Originator IPs.
Last 10 Information Interception Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This data monitor shows the last 10 Information Interception events.

Top Information Interception Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This data monitor displays a bar chart of the attacker addresses and priorities for information interception events.
Top Information Interception Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This data monitor displays a bar chart of thetargets and priorities for information interception events.
Severe Honeypot Events per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	Shows a moving average of severe honeypots event. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Top Attacker Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This data monitor shows the top honeypot attacker countries.
Top Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This data monitor shows the top honeypot attackers
Top Signatures	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This data monitor shows the top honeypot signatures.
Top Target Ports	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This data monitor shows the top honeypot target ports.
Last 20 Insecure Cryptographic Storage Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Provides real-time display of the last 20 insecure cryptographic storage events.
Top 10 Insecure Cryptographic Storage Assets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Shows real-time display of the top 10 assets with insecure cryptographic storage events.

Last 10 Meltdown|Spectre Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	This data monitor displays the last 10 Meltdown|Spectre vulnerabilities.
Last State Meltdown|Spectre Vulnerability Overview	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	Shows real-time display of the last 20 Meltdown|Spectre vulnerabilities related to assets and their compliance status.
Anti-Virus Stopped or Paused Events per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows a moving average of anti-virus stopped or paused event. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Last 10 Anti-Virus Stopped or Paused Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	This data monitor displays the last 10 anti-virus stopped or paused events.
Last 10 Failed Anti-Virus Signature Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	This data monitor displays the last 10 failed anti-virus signature events
Top 10 Assets with Anti-Virus Stopped or Paused Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows the top 10 assets with anti-virus stopped or paused events.
Top 10 Assets with Failed Anti-Virus Signature Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows the top 10 assets with failed anti-virus signature events.
Last 10 Malware Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows the last 10 Malware Activity events.
Last 10 Worm Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This data monitor displays the last 10 worm events.

Malware Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows the malicious code activity between Attacker-Target pairs.
Top 10 Malware Attacker Addresses	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malware attacker addresses.
Top 10 Malware Attacker Countries	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malware attacker countries.
Top 10 Malware Attacker Zones	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malware attacker zones.
Top 10 Malware Target Hosts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malware targets.
Top 10 Malware Target Zones	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malware targets.
Top 10 Malwares	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides a list of the top 10 malwares
Worm Activity per 10 Minutes	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a moving average of worm event. It displays data for the last hour and will generate a correlation event if the moving average is increased by 500%.
Worm Propagation - Event Graph	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This data monitor shows connection between attacker and target machines as they appear in worm events.

Botnet Activity - GeoView	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor shows all botnet events on a world map. Before using this data monitorplease make sure the following rule : Possible Botnet Activity is enabled and deployed
Last 10 Botnet Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor displays the last 10 botnet events.
Last 10 Phishing Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor displays the last 10 phishing events.
Top 10 Botnet Activity	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor shows the top 10 botnet activity.
Top 10 Phishing Attackers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor shows the top 10 Phishing attackers.
Top 10 Phishing Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This data monitor shows the top 10 phishing targets.
Last 10 Spam Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This data monitor displays the last 10 spam events.
Top 10 Spam Receivers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This data monitor shows the top 10 spam targets.
Top 10 Spammers	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This data monitor shows the top 10 Spammers.

Last 10 Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides a list of the last 10 successful logins across your assets categorized in development network domain.
Last 10 Traffic to Development from other Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides the last 10 Traffic to development from other network Domains
Last 10 Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides a list of the last 10 unsuccessful logins across your assets categorized in development domain.
Top 10 Hosts with Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides a list of the top 10 development hosts with most successful logins.
Top 10 Hosts with Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides a list of the top 10 development hosts with most unsuccessful logins.
Top 10 Traffic to Development from other Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This data monitor provides the top10 Traffic to Development from other Network Domains.
Compliance Risk Score Overview	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/	This data monitor displays an icon indicating the compliance risk score for each regulation section. The compliance score is maintained in the Compliance Score active list, and is calculated based on the severity of the rules that were triggered in the solution package.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AC/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.

Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AC/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AC/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AC/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AT/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AT/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AT/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AT/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AU/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AU/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AU/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-AU/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.

Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CM/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CM/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CM/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CM/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CP/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CP/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CP/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-CP/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.

Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IP/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IP/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IP/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IP/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IR/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IR/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IR/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-IR/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.

Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MP/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MP/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MP/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-MP/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PE/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PE/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PE/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PE/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PL/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.

Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PL/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PL/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PL/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PM/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PM/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PM/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PM/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PS/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PS/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PS/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-PS/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-RA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-RA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.

Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-RA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-RA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SA/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SA/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SA/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SA/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SC/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SC/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SC/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SC/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Last 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SI/	This data monitor shows a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SI/	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Top 20 Rules Fired	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SI/	This data monitor displays a graphic distribution of the 20 most frequently firing correlation rules of this section.

Top 20 Targets in Rule Firings	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/Overview/NIST-SI/	This data monitor shows which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.
Asset Inventory	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows event fields relevant to asset inventory type of events.
Audit Tool Logins	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows logins from remote machines to the audit tool.
Device Configuration Changes	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	Includes device fields.
Event with Attacker Data	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows the attacker fields.
Events with Target Assets	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows events which are related to target assets.
High Risk Events	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows event fields relevant to high risk events.
Inter-Domain Traffic	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows the assets involved in inter-domain communications.
Login Events	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows event fields relevant to login type of events.
Physical Security	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	A field set that can be used to show the relevant fields for physical security events.
Traffic Between Network Domains	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set shows events which are related to traffic between network domains.
User Authentication	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	This field set is used by an active channel to display all user authentication related events.
Vulnerability Fields	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	Includes the vulnerability fields.
Access Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies access attempts other than logins.
Administrative User	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	The purpose of this filter is identify events with administrative users. These events are defined as such in which either the source or destination users are administrative users. Administrative accounts have to be defined *in all lower case* in the active list Administrative Accounts.
Attacker Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	Identifies classified attacker assets.

Attacker Asset is Production	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for events originated from production assets.
Attacker Asset is Remote	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are originated from remote assets.
Attacker Asset is Third Party	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are originated from third party assets.
Attacker Asset is VOIP	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are originated from VOIP assets.
Attacker Asset is Wireless	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for events originated from wireless devices .
Attacker Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	Identifies non classified attacker assets.
Internal Attackers	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for events coming from systems inside the organization network.
Internal Targets	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for events targeting systems inside the organization network.
Target Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	Identifies classified target assets.
Target Asset is Critical	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are targeting highly critical assets.
Target Asset is Database	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter selects events targeting database hosts.
Target Asset is Development	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for eventstargeting development assets.
Target Asset is High Impact System	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are targeting highly critical assets.
Target Asset is PII	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter selects events targeting PII hosts.

Target Asset is Production	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for eventstargetingproduction assets.
Target Asset is Publcing Facing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are targeting Public Facing Assets.
Target Asset is Third Party	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter identifies events that are targeting third party assets.
Target Asset is VOIP	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter selects events targeting VOIP Assets.
Target Asset is Wireless	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	This filter looks for events targeting wireless devices .
Target Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	Identifies non classified target assets.
Attacker Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter checks whether the attacker asset is categorized under the Network Domains category.
Attacker Host or Address Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.
Attacker User Is Administrator	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter checks whether the attacker user is an administrator.
Attacker User Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events that have the Attacker User Name event fields populated.
Attacker or Target User Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events that have either the Attacker User Name or Target User Nameevent fields populated.
Attacks and Suspicious Activity	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.
Administrative Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	The purpose of this filter is to identify login attempts by administrative users. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Local Logins	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies local login events to a MS Windows or UNIX system.

Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.
Logouts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies all logout events. Change the conditions in this filter to match logout events from non-Windows systems.
Successful Administrative Login	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies successful logins by administrators.
Successful Administrative Logout	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies events that indicate successful administrative logouts from assets categorized in one of your Network Domains.
Successful Logins	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies successful logins by both administrative and non-administrative users.
Successful Logouts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies successful logouts by both administrative and non-administrative users.
Successful User Login	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies successful logins by non-administrative users.
Successful User Logout	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies events that indicate successful logouts by non-administrative users.
Unsuccessful Administrative Login	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies events that indicate unsuccessful administrative logins.
Unsuccessful Logins	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identified failed logins by both administrative and non-administrative users.
Unsuccessful User Login	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter identifies failed logins by non-administrative users.
User Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Authentication/	This filter selects any attempts at logging into systems by non-administrative users. It excludes machine logins into Microsoft Windows systems.
Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter shows all events going to or coming from machines which are categorized with the Site Asset Categories/Classification category.
File Creations	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Files/	This filter identifies created files.

File Deletions	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Files/	This filter identifies deleted files.
File Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Files/	This filter identifies all file changes.
Firewall Accepts	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Firewall/	This filter selects all events where a firewall granted passage to traffic.
Firewall Deny	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Firewall/	This filter selects events where a firewall denied passage to traffic.
Inbound Events	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter looks for events coming from outside the organization network targeting internal networks .
All Information Leak Events	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Information Leakage/	This filter selects events that reflect information leakage.
Organizational Records Information Leak	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Information Leakage/	This filter identifies information leaks with regard to company information.
Personal Records Information Leak	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Information Leakage/	This filter identifies information leaks with regard to personalinformation.
Insecure Services	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	Selects events based on inherently insecure services.
Insignificant Events	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter is used to identify events with no or little value. Preferably, these events should be filtered out by the connector.
Internal Connection	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter is looking for connections within the network.
Non Administrative User	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	The purpose of this filter is identify events associated with non-administrative users. These events are defined as such in which neither the source nor destination users are administrative users.
Outbound Events	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter looks for events coming from inside the organization network targeting the public network.

Compliance Score Updates	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Risk Score Dashboard Overview/	This filter identifies events that are generated when values in the Compliance Score active list are changed.
FISMA Rule Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Risk Score Dashboard Overview/	This filter selects all rule firing events, where the rule is a part of thecompliance content. This filter is used by the overview last-state data monitors. Also, the filter contains an exclusion list for the rules that should not contribute to the overall state as intended to be shown by the overview data monitor.
NIST-AC Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-AT Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-AU Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-CA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-CM Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-CP Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-IA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-IP Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.

NIST-IR Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-MA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-MP Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-PA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-PE Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-PL Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-PM Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-PS Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-RA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-SA Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
NIST-SC Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.

NIST-SI Rules Firing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Overview/Sections Overview/	This filter selects events generated by any rule firing in this section.
Policy Breaches	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	Filter in events with breach of policy.
Policy Violations	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	Filter in events with violation of policy.
Port Detected	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Ports/	Selects events indicating that port is detected
Recon Activity	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Recon/	This filter identifies events which indicate reconnaissance.
Successful Access	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies successful access other than logins. E.g. database query.
Target Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter checks whether the target asset is categorized under the Network Domains category.
Target Host or Address Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events that have either the Target Host Name or Target Address event fields populated.
Target MAC Address Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies events that have the Target MAC Address event fields populated.
Target User Present	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter checks whether the Target User Name field is populated.
Unauthorized Access of Information	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filter identifies unauthorized access of an object such as a file.
Vulnerability Events by Non-Scanners	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Vulnerabilities/	This filter identifies vulnerability events reported by non-scanner devices.
Vulnerability Scanner Events	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Vulnerabilities/	This filter identifies scanner-generated events.
Windows Events with a Non-Machine User	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	This filters identified Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.
After Hours	Filter	/All Filters/ArcSight Solutions/FISMA/My Filters/	This filter defines the time period of 'after hours'. Change this filter to adjust the default settings.

Event Limit	Filter	/All Filters/ArcSight Solutions/FISMA/My Filters/	The purpose of this filter is to limit events processed and reported by the solution pack to only the events that are relevant to the regulation. This is achieved by including this filter in the conditions of all other resources in the package such as rules, queries, and filters etc either directly or indirectly. You can change the events processed and reported by this package by editing this filter. See the solution guide for more information.
Limit Regulation	Filter	/All Filters/ArcSight Solutions/FISMA/My Filters/	The purpose of this filter is to ensure that the solution only processes events that are addressed by the regulation.
Access Rights Changes	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Selects events where a change was attempted for account access rights.
Account Creation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies account creation events.
Account Creations, Modifications and Deletions	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies all account management events.
Account Deletion	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies account deletion events.
Account Modification	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies account modification events.
Disabled Account Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This filter selects events that identify a disabled employee account. it's based on windows account disabled event "4725" , This filter require additional configurations by adding the organizational active directory Domains to Active Directory Domains Active List.
Enabled Account Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This filter selects events that identify when employee account is enabled. It's based on windows account enabled event "4722" , This filter requires additional configurations by adding the organizational active directory Domains to Active Directory Domains Active List.

Former Employee Account Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This filter selects events that identify a former employee account. It's based on windows account deleted event "4726" , This filter require additional configurations by adding the organizationalactive directory Domains to Active Directory Domains Active List.
Former Employee Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This filter identifies base events associated with users who are known to be terminated according to the Former Employees active list.
Login Activity by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This filter identifies login activities by accounts that are on the Stale Accounts active list.
Privileged Account Changes	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Selects events where a change is attempted to a privileged account (as defined by the referenced active list).
Removal of Access Rights	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies events indicating a user access right is removed.
Suspicious Activities by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies suspicious activities by accounts that are on the Stale Accounts active list.
User Added to Group	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies when an user is added to a group.
User Group Creation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies user group creation events.
User Group Deletion	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies user group deletion events.
User Group Modification	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies user group modification events.

User Removed from Group	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies when a user removed from group.
Login Activity from Non Classified Machines to Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	This filter shows all login activity from non-classified machines to classified machines.
Attacks from Non Classified Machines to Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter shows all attacks from non-classified machines to classified machines.
High to Low Classified Traffic Information Leak	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter looks for information leak events which originated from a high-security classified system.
Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter identifies events going from an asset in a higher classification level to an asset in a lower classification level.
Internal Inter-Domain Traffic	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter identifies internal inter-domain traffic.
Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter identifies events going from an asset in a lower classification level to an asset in a higher classification level.
Traffic Between Network Zones	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter detects events in which the attacker zone is different than the target zone.
Traffic from Classified Machines to Non Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter shows all traffic from classified machines to non-classified machines.
Traffic from Dark Address Space	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter detects events that are coming from the Dark Address Space.

Traffic from Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter identifies events going from an asset in a higher classification level to an asset in a lower classification level.
Traffic from Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter identifies events going from an asset in a lower classification level to an asset in a higher classification level.
Traffic from Non Classified Machines to Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter shows all traffic from non-classified machines to classified machines.
Traffic to Dark Address Space	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter detects events that are targeting the Dark Address Space.
Traffic to and from Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This filter shows all events going to or coming from machines which are categorized with the Site Asset Categories/Classification category.
Attacker is Custom Account	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This filter detects development, test, or custom application or user accounts in a source.
Communications between Development and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This filter identifies traffic between Development and Operations domains.
Communications between Development and Test	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This filter identifies traffic between Development and Test domains.
Communications between Test and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This filter identifies traffic between Test and Operations domains.
Target is Custom Account	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This filter detects development, test, or custom application or user accounts in a destination.

Special privileges assigned to new logon	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 6 Least Privilege/	This filters selects events which identifies when a special privileges assigned to new logon. it's based on windows event "4672" , This filter require additional configurations by adding the organizational active directory Domains to Active Directory Domains Active List.
Account Lockouts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This filter is used to identify account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.
All Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies all types of Brute Force Login Attempts.
Application Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies all application brute force login attempt events.
IDS Detected Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows events sent by Intrusion Detection Systems that indicate brute force login attempts.
IDS Detected Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Selects events from Intrusion Detection Systems that indicate a successful brute force login has occurred.
Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies events generated by the Probable Successful Brute Force rule that involve assets categorized in one of your Network Domains.
Workstation is Locked	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	This filter is used to identify when a workstation is locked, it's based on windows events.
Workstation is Unlocked	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	This filter is used to identify when a workstation is unlocked, it's based on windows events.
RDP Session Initiated	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	This filter is used to identify when an RDP Session is initiated.

RDP Session Terminated	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	This filter is used to identify when an RDP Session is terminated.
Outbound Internet Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	This filter detects all outbound internet activity related events.
Disallowed Ports Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Tracks all connections to disallowed ports.
Disallowed Ports Access from Internal Hosts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Tracks all connections to disallowed ports from internal hosts.
Disallowed Ports Access to Internal Hosts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Tracks all connections to disallowed ports hosted by internal hosts.
Non VPN Remote Access Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This purpose of this filter is to identify non-VPN remote access attempts.
Privileged Access on a Remote Connection	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This filter selects events where a connection is reported by a VPN device, and the user name belongs to a privileged account.
Successful Non VPN Remote Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This purpose of this filter is to identify successful non-VPN remote access.
Unsuccessful VPN Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This filter identifies failed VPN access attempts.
VPN Access Attempt	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This filter identifies VPN access attempts.

VPN Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Selects events indicating that a VPN configuration change has occurred.
AirDefense Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events from an AirDefense device.
AirMagnet Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events from an AirMagnet device.
AirPatrol Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events from an AirPatrol device.
Attacks and Suspicious Activity Targeting Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies attack and suspicious activity events that target assets or zones categorized in the Wireless asset category.
Attacks and Suspicious Activity from Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies attack and suspicious activity events from assets or zones that are categorized in the Wireless asset category.
Attacks and Suspicious Activity to and from Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Wireless asset category.
Rogue Station Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events when a rogue (unauthorized) station is detected.
Wireless Anomalous Traffic or Device Misconfiguration Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events where a wireless Intrusion Detection System (IDS) reports a traffic anomaly or a device misconfiguration.

Wireless Encryption Violation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events where a wireless Intrusion Detection System (IDS) reports a wireless traffic encryption violation.
Wireless Intrusion Detection Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events reported by a wireless Intrusion Detection System (IDS).
Wireless Malicious Traffic Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This filter identifies events where malicious wireless traffic is observed.
Attacks and Suspicious Activity Targeting Third Party Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This filter identifies attack and suspicious activity events targeting assets or zones categorized in the Third Party asset category.
Attacks and Suspicious Activity from Third Party Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This filter identifies attack and suspicious activity events that are generated by assets categorized in the Third Party asset category.
Attacks and Suspicious Activity to and from Third Party Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This filter identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Third Party asset category.
Removable Media Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This filter selects events indicating that a removable device is detected.
Removable Media Detected on Highly Critical Machine	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This filter selects events indicating that a removable device is detected on highly critical machine.
Successful Administrative Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify successful logins with an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.

Successful Administrative Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify successful logins with an administrative account to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Successful User Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify successful non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Successful User Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify successful non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Unsuccessful Administrative Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify failed logins using an administrative account from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Unsuccessful Administrative Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify failed administrative logins to Third Party Assets.Third Party systems have to be modeled as assets in ESM and be categorizes as Third Party. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Unsuccessful User Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify failed non-administrative logins from third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Unsuccessful User Logins to Third Party Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	The purpose of this filter is to identify failed non-administrative logins to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Third Party.
Possible Bitcoin Mining Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-23 Data Mining Protection/	This filter detects possible bitcoin mining activity using Nessus vulnerability scanner.

Assets with High Severity Vulnerability by Non-Scanners	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This filter selects events that indicate the existence of severe vulnerabilities reported by non-scanners.
Assets with High Severity Vulnerability by Scanners	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This filter selects events that indicate the existence of severe vulnerabilities reported by scanners.
Failed Technical Compliance Check	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This filter identifies events which indicate a compliance check failure.
External to Internal Traffic	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This filter selects events where the traffic originates from an external network segment and the target is in an internal network segment.
Internal to External Traffic	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This filter selects events where the traffic originates from an internal network segment and the target is in an external network segment.
Information System Failures	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This filter identifies information system failures.
Windows Domain Policy Changed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Selects events indicating that a Windows domain policy was changed.
Windows Group Policy Changed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Selects events indicating that a windows group policy was changed.

Resource Exhaustion	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).
Security Log is Full	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	The security log is now full.
FISMA Reports Generation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Filter events where a FISMA report is generated.
Unable to Log Events to Security Log	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Shows events indicating inability to log events to security log.
Big Difference Between End Time and Manager Receipt Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This filters identifies time discrepancies between endTime and managerReceiptTime. By default it will identify events with a difference of more than 600 seconds (10 minutes).
Clock Synchronization Issues	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This filter identifies different kinds of clock synchronization issues.
Device Time is Later than Agent Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This filter identified events in which the device receipt time is after the agent receipt time. By default it will show events for which the device receipt time is more than 300 seconds (5 minutes) than the agent (connector) receipt time.
Audit Log Cleared	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Selects all events where an audit log was cleared from a host. By default it will recognize events on Microsoft Windows and Symantec Host IDS systems, modify this filter to include events from other devices.
Audit Log Cleared Rule Fired	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Detects correlated eventsthe rule Audit Log Cleared generates.

Information System Audit Tool Login	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This filter identifies logins to information system audit tools. By default it shows only logins to ArcSight products.
Failed Administrative Actions	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This filter identifies failed administrative actions.
Failed User Actions	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This filter identifies failed non administrative actions.
Successful Administrative Actions	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This filter identifies successful administrative actions.
Successful User Actions	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This filter identifies successful non administrative actions.
Information Disclosure Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	Selects events indicating that an information disclosure vulnerability was detected.
Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Detects non-arcsight configuration modifications events.
Database Configuration Modification	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Detects database configuration modifications.
Firewall Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks events when the configuration of a firewall is changed.

Network Device Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks events when the configuration of an infrastructural equipment (router, switch) is changed.
Network IDS Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks events when the configuration of NIDS equipment is changed.
Network Routing Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Tracks events when a modification to the routing table of infrastructural equipment (router, switch) is made.
Operating Systems Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Identifies successful configuration modifications to operating systems.
Unsuccessful Operating Systems Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Identifies unsuccessful changes attempted on operating systems.
Asset Creation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Select events indicating the creation of a new asset.
Asset Deletion	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Select events indicating the deletion of an asset.
Asset Modification	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Select events indicating the modification of an asset.
Nessus Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This filter selects all events from a Nessus scanner.

New Host Creation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This filter selects events which indicate that new hosts were detected on the network. Normally reported by network based anomaly detection systems (NBAD).
New Service Creation	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This filter selects events which indicate that new services were created on a host.
Software Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This filter selects events when a new piece of software (except operating systems) is detected by a scanner.
eEye Retina Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This filter selects all events from an eEYE Retina scanner.
Shutdown Machine not Started more than Policy Standard	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This filter identifies shutdown machines not started more than policy standard.
System Shutdown	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This filter identifies system shut downs.
System Shutdown of Highly Critical Assets	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This filter identifies system shut downs of highly critical assets.
System Startup	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This filter identifies system startups.
Default Vendor Account Access Attempted	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Identifies events where system access with vendor-supplied accounts is attempted.

Default Vendor Account Credential Observed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Identifies events where system access with vendor-supplied accounts is observed.
Direct Root or Administrator Credential Observed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Identifies events where system access with root or administrator credential is observed.
Non Multi Factor Access by Admin Account	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This filter detects events indicating a non multi factor authentication to CDE by admin accounts.
Replay Attack was Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Identifies events when a Microsoft windows replay attack is detected.
Accepted Accesses Through AAA Server	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects all the accepted accesses through AAA Server.
All DHCP Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects events from all DHCP servers available in the system.
DHCP Critical Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter identifies critical events related to a DHCP server.

DHCP Critical Logging Errors	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects critical logging errors from all DHCP servers in the system.
DHCP Lease Assigned or Renewed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects events when a DHCP server in the system leases out (or extends) an IP address to a client.
DHCP Lease Expired or Released	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects events when a DHCP client releases its IP or fails to extend its current lease.
Rejected Accesses Through AAA Server	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects all the rejected accesses through AAA server .
Unix DHCP Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects all events from Unix DHCP servers.
Unix DHCP Events from a Client	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects all events from a client to a Unix DHCP server.
Windows DHCP Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This filter selects all events from Windows DHCP servers.

Failed Password Change	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Identifies unsuccessful password change events.
Password Change Attempts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Identifies password change attempts. By default it only identifies these events on Microsoft Windows systems. Configure this filter to identify password change events from other systems as necessary.
Password Policy modified	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Identifies when a password policy change happens.
Successful Password Change	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Identifies successful password change events.
FISMA Case Created	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This filter identifies events where a new case is created.
Attacks with Geo Information	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This filter selects attack events with populated Geo fields for both the attacker and target addresses.
Compromises	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This filter identifies generic compromises.
High Priority Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This filter shows events in which the Priority field is 10.
Internal Recon Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This filter identifies events which indicate internal reconnaissance.
Reconnaissance - Geo Information	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This filter identifies reconnaissance events in which the Geo information fields are populated for both attacker and target.

Critical Machine Configuration Modifications at Unscheduled Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	Identifies successful configuration modifications to critical machineoutside the maintenance window.
Maintenance Window	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This filter defines what is considered outside of maintenance window(s). Change this filter to adjust the default settings - Sunday morning, 3:00 AM to 3:59 AM, and Wednesday morning, 4:00 AM to 4:59 AM. Reminders for variables: For HourOfDay, 3:00 PM = 15, i.e. 24 hours style.
Network Device Configuration Modifications at Unscheduled Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	Tracks events when the configuration of an infrastructural equipment (router, switch) is changed outside the maintenance window.
System Shutdown or Restart at Unscheduled Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This filter detects system shutdown or restart outside the maintenance window.
Unscheduled Change in Status of Service	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This filter selects events any time a service on a host is changed when it is outside of a scheduled maintenance window. The maintenance window is defined by the referenced filter.
Monitored Accounts Email Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This filter identified email activity by monitored users .
Successful Monitored Account Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This filter identified successful login attempts by monitored users .
Suspicious Activity by Monitored Accounts	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This filter identified suspicious activity performed by monitored accounts.
Unsuccessful Monitored Accounts Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This filter identified unsuccessful login attempts by monitored users .

Badge Out	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies badge out event.
Building Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	This filter selects all building access events.
Contractor Access After Hours	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies contractors accessing buildings after hours.
Physical Access Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Selects all events sent to ArcSight ESM by physical security systems.
Successful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Selects all events indicating successful occurrences of physical access after business hours. The actual time definition is defined in the After Hours filter.
Successful Badge In	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies a successful badge-in event.
Successful Building Access Granting	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies granting user access to a building.
Unsuccessful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Selects all events indicating unsuccessful occurrences of physical access after business hours. The actual time definition is defined in the After Hours filter.
Unsuccessful Badge In	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies an unsuccessful badge-in event.

Email Traffic	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies generic email traffic.
Former Employee Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies the outbound internet activity of former employees. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Monitored Accounts Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies the outbound internet activity of monitored users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
New Hire Account Added to Group	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies when a new hire account added to group.
New Hire Account Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter selects events that identify a new hire employee account. it's based on windows account deleted event "4720" , This filter require additional configurations by adding the organizational active directory Domains to Active Directory Domains Active List.
New Hire Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies the outbound internet activity of new hire users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
New Hire Suspicious Activities	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies suspicious activity by new hires.
New Hires Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identified login attempts by new hire users .
New Hires Successful Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identified successful logins by new hire users .
New Hires Unsuccessful Logins	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identified unsuccessful logins by new hire users .

Non Privileged Accounts Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies the outbound internet activity of non privileged accounts. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Privileged Accounts Based Internet Outbound Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This filter identifies the outbound internet activity of privileged accounts. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Information Disclosure Vulnerability Detected on PII Asset	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Selects events indicating that an information disclosure vulnerability was detected on PII assets.
Insider Threat	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This filter identifies events which originated from internal assets against internal assets.
Critical Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that a critical vulnerability was detected.
Overflow Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that an overflow vulnerability detected.
SQL Injection Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that SQL injection vulnerability was detected.
Security Patch Missing	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that a security patch is missing.
XSRF Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that an XSRF vulnerability was detected.
XSS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Selects events indicating that an XSS vulnerability was detected.

DoS Attacks	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This filter identifies denial of service attacks.
Traffic Anomaly	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This filter detects events indicating a taffic anomaly.
Traffic Anomaly on Application Layer	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This filter detects events indicating a taffic anomaly on application layer
Traffic Anomaly on Network Layer	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This filter detects events indicating traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This filter detects events indicating traffic anomaly in transport layer .
Cryptographic Hash Algorithm Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Cryptographic Public Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating thatpotential symmetric key related vulnerability was detected.

Cryptographic Weak Protocol Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
SSH Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that an SSH vulnerability was detected.
SSL|TLS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that an SSL/TLS vulnerability was detected.
VPN Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that a VPN vulnerability was detected.
Invalid or Expired Certificate	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Selects events which indicate that an invalid or expired certificate was detected.
Mobile Code Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-18 Mobile Code/	Detects mobile code applications, by default the detection is based on Nessus and Snort products.
SIP 4XX Response	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Selects events indicating sip 4xx response,its based on snort.
VOIP Application Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Selects events indicating that VOIP application was detected.
VOIP Attacks and Suspicious Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This filter identifies voip events which indicate compromise, reconnaissance, hostile, or suspicious activity reported from various devices.

VOIP Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Selects events indicating that VOIP application was detected.
VOIP Ghost Call Attack	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Selects events indicating that a VOIP Ghost call attack was detected ,its based on snort.
VOIP Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Selects events indicating that an VOIP vulnerability was detected.
DNS Bind Query	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Selects dns bind queries events.
Information Interception	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This filter detects events indicating an information interception is being used.
Redirection Attacks	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This filter detects events indicating a redirection attack occurred.
Honeypot Interaction Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This filter detects honeypots events, by default it based on modern honey network events (https://github.com/threatstream/mhn) ,for adding other honeypots the user need to customize this filter.
Severe Honeypot Events	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This filter detects severe Honeypot Events, by default it based on modern honey network events (https://github.com/threatstream/mhn) ,for adding other honeypots the user need to customize this filter.

Insecure Cryptographic Storage Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Selects events indicating that Insecure cryptographic storage has been detected.
Covert Channel	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-31 Covert Channel Analysis/	This filter detects events indicating a covert channel is being used.
Meltdown|Spectre Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	Detects Meltdown and Spectre Vulnerabilities.
Anti-Virus Service Stopped or Paused	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Selects events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.
Anti-Virus Service Stopped or Paused in Windows	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Selects Windows events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.
Failed Anti-Virus Updates	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Looks for events when an attempt to update a virus signature on a host failed.
Anti-Virus Clean or Quarantine Attempt	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Looks for anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.
Failed Virus Removal Attempt	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Looks for events when an attempt to remove/quarantine a virus on a host failed.
HTTP Request	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Looks for HTTP Requests.

Malware Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Selects events where malicious code activity is detected.
Potential Trojan Inside Network	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Selects events where a trojan is likely to be present inside the company network.
Shell Code Execution Detected	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Selects events where shellCode execution is detected.
Spyware Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Trojan Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Selects events where trojan activity is detected.
Virus Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Identifies virus activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Worm Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Selects events where worm activity is detected.
Botnet Activity	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This filter detects events indicating a botnet activity, it's based on this rule Possible Botnet Activity.
Email Attacks	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This filter detects events indicating an email attack (like phishing,spam..) occurred.

Email Traffic with Competitors	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This filter identifies email traffic with competitor companies.
Phishing Attacks	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This filter detects events indicating an phishing attack occurred.
Windows Service Installed	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This filter detects events indicating a windows service was installed.
BIOS Flaws	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This filter detects events indicating a Basic Input Output System (BIOS) flaws.
Spamming Attacks	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This filter detects events indicating an email spam sent.
ASLR or Data Execution Prevention Bypass Flaws	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Selects events indicating that an ASLR or Data Execution Prevention Bypass Flaw detected.
Data Execution Prevention (DEP) is Disabled	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Selects events indicating that a data execution prevention is disabled , this filter is based on Nessus signature id 24282.
File Changes in Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This filter identifies all file changes on development environment.

Successful Administrative Logins to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	The purpose of this filter is to identify successful logins with an administrative account to third party systems. Third party systems have to be modeled as assets in ESM and be categorizes as Development. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Successful Logins to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This filter identified successful logins by both administrative and non-administrative users to development domain.
Successful User Logins to Development Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	The purpose of this filter is to identify successful non-administrative logins to Development systems. Development systems have to be modeled as assets in ESM and be categorizes as Development.
Traffic from Others to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Selects all traffic destined for the development segment(s) of the network that did not originate from within a development segment.
Unsuccessful Administrative Logins to Development Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	The purpose of this filter is to identify failed administrative logins to Development.Development systems have to be modeled as assets in ESM and be categorizes as Development. Administrative accounts should be defined in all-lower case in the Administrative Accounts active list.
Unsuccessful Logins to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This filter identified unsuccessful logins by both administrative and non-administrative users to development domain.
Unsuccessful User Logins to Development Systems	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	The purpose of this filter is to identify failed non-administrative logins to Development systems. Development systems have to be modeled as assets in ESM and be categorizes as Development.

Account Creations in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This reports shows all account creations in production.
Account Deletions in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This reports shows all account deletions in production.
Account Modifications in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This reports shows all account modifications in production.
Communication between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communication between assets in those 2 network domains development and third party .
Communication between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communication between production and third party assets.
Communication between Third Party and Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communication between secret machines and third party assets.
Communication between Third Party and Top Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communication between top secret machines and third party assets.
Communication between Third Party and Unclassified Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communication between unclassified machines and third party assets.
Successful Administrative Logins between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows successful administrative logins with an administrator account between assets in those 2 network domains development and third party .

Successful Administrative Logins between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows successful administrative logins with an administrator account between assets in those 2 network domains production and third party .
Communication between Financial Assets and Public Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows communication between financial and public facing assets.
Communication between Production and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows communication between production and development assets.
Communication between Test and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows communication between Test and Development
Successful Administrative Logins between Development and Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows successful administrative logins between development and production.
Suspicious Activity on Financial Systems from Machines not in the Financial Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows all suspicious activity to systems in a financial Domain from systems not in that domain.
Suspicious Activity on HR Systems from Machines not in the HR Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	This report shows all suspicious activity to systems in a HR Domain from systems not in that domain.
Resource Exhaustion Detected on Critical Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on critical systems.

Resource Exhaustion Detected on Processing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on processing systems.
Resource Exhaustion Detected on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on production domain.
Resource Exhaustion Detected on Public Facing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on public facing systems.
Resource Exhaustion Detected on Third Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on third party accessible assets.
Organizational Information Leaks on Databases	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on databases, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Organizational Information Leaks on Legal Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on legal systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Organizational Information Leaks on Processing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on processing systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.

Organizational Information Leaks on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on production systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Organizational Information Leaks on Public-Facing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on public facing systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Organizational Information Leaks on Third-Party Accessible Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on third party accessible systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Personal Information Leaks on Commerce Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak oncommerce systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Personal Information Leaks on Databases	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on databases, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Personal Information Leaks on Electronic PII	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on electronic PII, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.

Personal Information Leaks on Email Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on email systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Personal Information Leaks on Financial Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on financial systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Personal Information Leaks on HR Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on HR systems, Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Configuration Modifications in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to development network domain.
Configuration Modifications in Email Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to email network domain.
Configuration Modifications in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to production network domain.
Configuration Modifications in Public-Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to public-facing network domain.
Configuration Modifications in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to test network domain.

Configuration Modifications in Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to third party accessible assets.
Configuration Modifications in Wireless Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to wireless network domain.
Vulnerabilities Summary on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 4 Security and Privacy Impact Analysis/	Provides overview of vulnerability summary reported by vulnerability scanners on test environment on the last day.
Account Change Details in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events when an account was attempted to be changed on development network domain.
Account Change Details in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events when an account was attempted to be changed on production network domain.
Account Change Details in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events when an account was attempted to be changed on test network domain.
Successful Removal of Access Rights in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This report shows the removal of access rights from a host resource in a development environment.
Successful Removal of Access Rights in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This report shows the removal of access rights from a host resource in a production environment.
Successful Removal of Access Rights in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This report shows the removal of access rights from a host resource in a test environment.

New Systems on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new development assets on the last month.
New Systems on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new production assets on the last month.
New Systems on Public-Facing Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new public-facing assets on the last month.
New Systems on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new test assets on the last month
New Systems on Third-Party Accessible Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new third-party accessible assets on the last month.
New Wireless Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new wireless assets on the last month.
Assets in FIPS-199 Availability Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets which categorized as FIPS-199 availability criticality.
Assets in FIPS-199 Conditionality Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets which categorized as FIPS-199 conditionality criticality.
Assets in FIPS-199 Integrity Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets which categorized as FIPS-199 integrity criticality.

Assets in NIST 800-53 High Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the NIST 800-53 high impact criticality domain.
Assets in NIST 800-53 Low Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the NIST 800-53 low impact criticality domain.
Assets in NIST 800-53 Moderate Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the NIST 800-53 moderate impact criticality domain.
Assets in the Development Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Development Network Domain.
Assets in the Operations Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Operation Network Domain.
Assets in the Production Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Production Network Domain.
Assets in the Public-Facing Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Public-Facing Network Domain.
Assets in the Test Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Test Network Domain.
Assets in the Third Party Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Third Party Domain.

DNS Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all of assets which categorized as DNS systems.
Database Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all of assets which categorized as databases.
Email Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Email Network Domain.
Financial assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Financial Network Domain.
Human Resources Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Human Resources Domain.
Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all of assets which categorized as PII.
Web Application Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all of assets which categorized as web applications.
Wireless Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of all the assets for the Wireless Network Domain.
Critical Asset Details on Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical development assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.

Critical Asset Details on Operations	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical operation assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Asset Details on Processing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical processing assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Asset Details on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical production assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Asset Details on Public-Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical public-facing assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Asset Details on Third-Party	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical third party assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Financial Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical financial assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Critical Wireless Components	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical wireless assets which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Shutdown of Critical Machines on Development Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on development network domain on the last day.
Shutdown of Critical Machines on Email Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on email network domain on the last day.

Shutdown of Critical Machines on Financial Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on financial network domain on the last day.
Shutdown of Critical Machines on Operations Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on operations network domain on the last day.
Shutdown of Critical Machines on Processing Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on processing network domain on the last day.
Shutdown of Critical Machines on Production Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on production network domain on the last day.
Shutdown of Critical Machines on Public-Facing Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on public-facing network domain on the last day.
Shutdown of Critical Machines on Third-Party Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on third-party network domain on the last day.
Shutdown of Critical Wireless Components	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on wireless network domain on the last day.
Attacks and Suspicious Activities from Afghanistan	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Afghanistan.
Attacks and Suspicious Activities from Brazil	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Brazil.
Attacks and Suspicious Activities from China	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from China.
Attacks and Suspicious Activities from Iran	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Iran.

Attacks and Suspicious Activities from Iraq	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Iraq.
Attacks and Suspicious Activities from Israel	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Israel.
Attacks and Suspicious Activities from North Korea	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from North Korea.
Attacks and Suspicious Activities from Russia	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Russia.
Attacks and Suspicious Activities from Syria	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from Syria.
Attacks and Suspicious Activities from USA	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from USA.
Reconnaissance Activities Targeting Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all reconnaissance activities targeting production.
Reconnaissance Activities Targeting Public-Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all reconnaissance activities targeting public-facing assets.
Successful Logins to Intellectual Property Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of successfullogin attempts to intellectual property records. assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Successful Logins to Patient Medical Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of successfullogin attempts to medical records. assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.

Unsuccessful Logins to Intellectual Property Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of unsuccessfullogin attempts to intellectual property records. assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Unsuccessful Logins to Patient Medical Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of unsuccessfullogin attempts to medical records.assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Reconnaissance Activities Targeting Electronic PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report shows a list of all reconnaissance activities targeting Electronic PII asstes.
Successful Logins to Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This Report shows all the successful logins to personal identification information assets on the last 24 hours.
Suspicious Activity on PII Assets from Machines from other Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report shows all attacks and suspicious activity to systems in a electronic PII domain from systems not in that domain.
Top 10 Vulnerable PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report provides information about the top 10 vulnerable PII assets.
Unsuccessful Logins to Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This Report shows all the unsuccessful logins to personal identification information assets on the last 24 hours.
Vulnerabilities Summary on PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Provides overview of vulnerability summary on PII assets.

Communication between Test Environment and PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	This report shows all the communication between Test environment and PII assets.
Cross-Talk Between Test Environment and PII Asset	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	This report shows all cross-talk in the last 24 hours between assets in test environment and PII assets.
Personal Information Leaks on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	This report shows all personal information leakage on test environment.
Successful Administrative Logins between Test Environment and PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	This report shows all successful administrative logins between test environment and PII Assets.
Configuration Modifications in Personal Identifiable Information Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-29 Inventory of Personally Identifiable Information/	Displays the changes were made to personal identifiable information systems.
New Personal Identifiable Information Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-29 Inventory of Personally Identifiable Information/	This report shows an overview of the new personal identifiable information assets on the last month.
Top 10 Vulnerable Assets on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable assets on the development environment.

Top 10 Vulnerable Assets on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable assets on the production environment.
Top 10 Vulnerable Assets on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable assets on the test environment.
Top 10 Vulnerable Critical Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable critical assets.
Top 10 Vulnerable Public Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable public-facing assets.
Top 10 Vulnerable Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This report provides information about the top 10 vulnerable third-party accessible assets.
Vulnerabilities Summary on Critical Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on critical assets on the last day.
Vulnerabilities Summary on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on development environment on the last day.
Vulnerabilities Summary on PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on PII assets on the last day.
Vulnerabilities Summary on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on production environment on the last day.
Vulnerabilities Summary on Public Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on public facing assets on the last day.
Vulnerabilities Summary on Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary reported by vulnerability scanners on third-party accessible assets on the last day.

Blocked Firewall Traffic from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the blocked outbound firewall traffic originating from third party systems.
Blocked Firewall Traffic to Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the blocked inbound firewall traffic directed at assets in third party domain.
Firewall Traffic from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the outbound firewall traffic originating from third party systems.
Firewall Traffic to Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the inbound firewall traffic directed at assets in third party domain.
Policy Violations Originated from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	Provides a listing of events categorized by ArcSight as policy violations which originated from the third party domain.
Policy Violations on Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	Provides a listing of events categorized by ArcSight as policy violations which target the third party domain.
VOIP Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Provides a listing of all the assets for the VOIP network Domain.
Configuration Changes in Third Party Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA- 9 External System Services/	Displays the changes were made to third party machines.

Account Creations in Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This reports shows all account creations in development domain.
Account Deletions in Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This reports shows all account deletions in development.
Account Modifications in Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This reports shows all account modifications in development.
Attacks and Suspicious Activities Targeting Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report shows a list of all attack and suspicious activity events targetingdevelopment.
Attempted File Changes in Development Originated from Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Displays attempts to change a file on a host in the development segment from a source that is in production.
Attempted File Changes in Development Originated from Test	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Displays attempts to change a file on a host in the development segment from a source that is in test.
Attempted File Changes in Development Originated from Third Party	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Displays attempts to change a file on a host in the development segment from a source that is in Third Party.
Account Creations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information System accounts that were created.

Account Creations in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Deletions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information System accounts that were deleted.
Account Deletions in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were deleted in a specific network domain. By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information System accounts that were modified.
Account Modifications by Attacker User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were modified by a specific user (default admin).
Account Modifications by Target User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all the modification of a specific information system account (default admin).
Account Modifications in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were modified in a specific network domain (default Development). By default, the Development network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Activity by Former Employees	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows any activity performed by users who are known to be terminated.

Disabled Privilege Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all the disabled privilege user accounts.
Disabled User Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all the disabled user accounts.
Enabled User Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all the enabled user accounts.
Failed or Attempted Removal of Access Rights	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all failed or attempted removal of access rights from a host resource.
Former Employee Account Access Attempt	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists all log-in activity from a former employee.
Former Employee Accounts in Use	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies all former employee user names and reporting device details associated with recent events.
Inactive User Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user names that are in the Stale Accounts active list.
Login Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows stale user accounts from which login activity was attempted.
Privileged Account Change Details	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists details of events regarding changes to privileged accounts.
Successful Removal of Access Rights	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all the removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
Suspicious Activities by Former Employee	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists all suspicious Activities by former employee.

Suspicious Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows suspicious activities of stale user accounts.
User Group Creations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information User Groups that were created.
User Group Deletions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information User Groups that were deleted.
User Group Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information User Groups that were modified.
Users Added or Removed from Group - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information of Users which added or removed from specific group.
Users Added to Groups	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information of Users which added to Groups.
Users Removed from Groups	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all Information of Users which removed from Groups.
Login Activity from Non Classified Machines to Classified Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Provides a listing of login activity from non classified machines to classified machines.
Login Activity to Critical Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Provides a listing of login activity to critical machines.
Unauthorized Access to High Impact Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Provides a listing of unauthorized accesses to high impact systems.

Access to Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query shows all successful accesses to systems in a certain Network Domain from machines not in that domain.
Attacks from Non Classified Machines to Classified Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Provides a listing of attacks from non classified machines to classified machines.
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.
High to Low Classified Asset Communication	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.
High to Low Classified Traffic Information Leak	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Provides a listing of information leak from classified machines to non-classified machines.
Low to High Classified Asset Communication	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.
Suspicious Activity on Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query shows all suspicious activity to systems in a certain Network Domain from machines not in that domain.
Traffic Between Zones	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query shows the target ports between zones.
Traffic from Classified Machines to Non Classified Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Provides a listing of traffic from classified machines to non classified machines

Traffic from Dark Address Space	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic from Non Classified Machines to Classified Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Provides a listing of traffic from non classified machines to classified machines.
Traffic to Dark Address Space	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This query shows all traffic directed to a dark address range. This should be considered very suspicious.
Attacks from Development Targeting Production	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides a listing of hostile or suspicious traffic from development machines targeting production facilities.
Attacks from Production Targeting Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides a listing of hostile or suspicious traffic from production facilities targeting development machines.
Development and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Returns all assets that implement multiple functionality, for example, a database and Web server installed on the same machine.
Operations and Development Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.
Operations and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides all cross-talk in the last 24 hours between assets in Operations category and assets in Test category.
Shared Machines among Test, Development and Operation	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Returns all assets that are shared between at least two of the Test, Development and Operation domains.

Test and Development Accounts in Production Environment	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This query retrieves test and development accounts which used in production environment.
Special privileges assigned to new logon	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 6 Least Privilege/	Provides a listing of special privileges assigned to new logon.
Account Lockouts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Retrieves all information about account lockouts.
Account Lockouts per System	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Retrieves a count of all the account lockouts per system during the last 24 hours.
Account Lockouts per User and System	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Counts account lockouts per user and system.
Application Brute Force Login Attempts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies all user names for which there are a continuous set of unsuccessful login attempts.
Frequent Unsuccessful Logins from Attacker Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.
Frequent Unsuccessful Logins to Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies all target hosts which have received a continuous set of unsuccessful login attempts.
Successful Brute Force Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Provides a listing of events categorized by ArcSight as probable successful brute-force login attempts.May (and should) be focused based on the Network Domain of interest.

Top Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows the topl unsuccessful user logins within the last day.
Top Unsuccessful User Logins by Attacker Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of topl unsuccessful user logins within the last day by specific attacker host (default localhost)
Top Unsuccessful User Logins by Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of topl unsuccessful user logins within the last day by specific target host (default localhost)
Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of all unsuccessful user logins within the last day.
Unsuccessful User Logins by Attacker Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of all unsuccessful user logins within the last day by specific attacker host (default localhost)
Unsuccessful User Logins by Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of all unsuccessful user logins within the last day by specific target host (default localhost)
Unsuccessful User Logins by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query shows details of all unsuccessful user logins within the last day by specific user (default admin)
Workstation Locked\Unlocked Events by User Name - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Retrieves all information about workstation locks by specific user, it's based on windows events.
Workstation Locked\Unlocked Events by Workstation - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Retrieves all information about workstation locks by workstation, it's based on windows events.
Workstation Locked\Unlocked Events by Workstation and User Name - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Retrieves all information about workstation locks by workstation and user name, it's based on windows events.

RDP Session is not Terminated for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	Lists RDP Sessions which was not changed for longer than the policy standard permits.
Bypassing Authentication or Authorization Flaw Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Retrieves all the bypassing authentication or authorization flaws Detected.
Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Displays all the identified outbound internet activity . Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Internet Activity by Attacker Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Displays all the identified outbound internet activity by attacker address (default 127.0.0.1) . Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Internet Activity by Target Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Displays all the identified outbound internet activity by target address (default 127.0.0.1) . Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Internet Activity by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Displays all the identified outbound internet activity by specific user (default admin) . Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
All VPN Access Attempts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows all VPN access attempts.
Attacks and Suspicious Activities from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query provides a listing of all hostile or suspicious events from assets categorized as Remote.
Disallowed Port Attempted or Failed Access Summary	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows attempt or failed access to disallowed ports.

Disallowed Ports	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows traffic that should not be seen per the Allowed Ports active list.
Disallowed Ports by Connection Types	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the top disallowed ports grouped by connection types.
Inbound Insecure Transmissions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Inbound Traffic	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query provides a count of inbound traffic.
Organizational Information Leaks Originated from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query shows events which indicate a organizational information leak originated from remote assets.
Personal Information Leaks Originated from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query shows events which indicate a personal information leak originated from remote assets.
Privileged VPN Remote Access Attempts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows all connections reported by a VPN device, where the user name belongs to a privileged account.
Reconnaissance from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query shows reconnaissance activity from assets in the Remote domain.
Successful Administrative Logins from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query retrieves successful logins with an administrator account from assets categorized as Remote.
Successful Non VPN Remote Accesses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists succesfull non VPN remote accesses.
Successful User Logins from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query retrieves successful logins using a non-administrative account, from assets categorized as Remote.

Successful VPN Access by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all successful VPN accesses by specific user ,The user has to be specified at report runtime (default admin).
Suspicious Activities to Disallowed Ports	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows suspicius traffic that should not be seen per the Allowed Ports active list.
Top Disallowed Ports	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the top disallowed ports.
Top Internal Hosts Accessed Disallowed Ports	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the top internal hosts that accessed most disallowed ports.
Top Internal Hosts Provided Disallowed Ports	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the top internal hosts that provided most disallowed ports.
Top VPN Devices with Most Successful Configuration Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows top VPN devices with most successful configuration modifications.
Unsuccessful Administrative Logins from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query retrieves failed logins using an administrative account, from assets categorized as Remote.
Unsuccessful User Logins from Remote Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This query retrieves failed logins using a non-administrative account, from assets categorized as Remote.
Unsuccessful VPN Access	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all failed VPN access attempts.
VPN Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows any configuration modifications of any VPN device. Default time window: Last 24 hours.

VPN Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows the top configuration modifications of any VPN device.
Bluetooth Protocol Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This query retrieves Bluetooth protocol related flaws reported by vulnerability scanners.
Count of Attacks and Suspicious Activity Event Names on Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This report counts the names of attack and suspicious activity events on a particular Network Domain.
Wireless Encryption Violations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	Returns all wireless encryption violations detected by a wireless Intrusion Detection System (IDS) in the last 24 hours.
Wireless Malicious Traffic	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This query returns all wireless malicious traffic detections by a wireless Intrusion Detection System (IDS) in the last 24 hours.
Wireless Security Protocol Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This query retrieves flaws reported by vulnerability scanners which related to wireless security protocols such as WEP,WPA,WPA2 etc..
Disallowed Port Attempted or Failed Access Summary from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report shows attempt or failed access to disallowed ports from third party systems.
Disallowed Port Successful Access Summary from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query shows successful access to disallowed ports from third party systems.
Removable Media Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours.
Removable Media Activity by Device ID - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours by specific device id.

Removable Media Activity by Host - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours by specific hostname (default localhost).
Removable Media Activity by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours by specific user (default admin).
Successful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves successful logins with an administrator account from assets categorized as Third Party.
Successful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query identifies successful logins with an administrative account to third party systems.
Successful User Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves successful logins using a non-administrative account, from assets categorized as Third Party.
Successful User Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves successful logins using a non-administrative account, to assets categorized as Third Party.
Third-Party Access	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query shows all access attempts to assets by third parties.
Unsuccessful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves failed logins using an administrative account, from assets categorized as Third Party.
Unsuccessful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves failed logins using an administrative account, to assets categorized as Third Party.
Unsuccessful User Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves failed logins using a non-administrative account, from assets categorized as Third Party.
Unsuccessful User Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This query retrieves failed logins with a non-administrator account to assets categorized as Third Party.

Possible Bitcoin Mining Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-23 Data Mining Protection/	This query retrieves possible bitcoin mining machines.
Assets that Failed Technical Compliance Check	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This query finds assets which failed the technical compliance check.
Attacks and Suspicious Activities Targeting Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query provides a listing of all hostile or suspicious events targeting third party assets sorted by the event's end time.
Attacks and Suspicious Activities from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query provides a listing of all hostile or suspicious events from third party assets sorted by the event's end time.
Communication between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query shows all access attempts between 2 network domains. default network domains : development and test.
External to Internal Traffic	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query provides a count of inbound traffic.
Internal to External Traffic	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query provides a count of outbound traffic.
Successful Administrative Logins between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This query retrieves successful administrative logins with an administrator account between assets in 2 network domains . default network domains : development and test.
Information System Failures	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This query retrieves the number of information failures per asset.

Penetration Testing not Performed for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA-8Penetration Testing/	This query retrieves assets which penetration testing not Performed for themlonger than policy standard.
Windows Domain Policy Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Lists all the changes to Microsoft Active Directory.
Windows Group Policy Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	This query lists all the changes to Microsoft Active Directory.
Windows System Audit Policy Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Shows all Windows system audit policy changes.
Events by Certain Object - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This query selects events by certain object (default /Host/Application).
Events by Device Group - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This query selects events by device group (default /Firewall).
Events by Outcome - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This query selects events by outcome.
Resource Exhaustion Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).
Resource Exhaustion Detected - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain) .

Security Log is Full	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	This query retrieves windows events when security log is full.
Syslog Restart Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Shows all restarts of syslog on systems.
Unable to Log Events to Security Log	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	This query retrieves windows events indicating inability to log events to security log.
Device Logging Review	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 6 Audit Review, Analysis, and Reporting/	This query shows the different products that are logging to ArcSight ESM.
Clock Synchronization Issues	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This query displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime.
Clock Synchronization Issues - Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This query displays a summary of the number of events for each device that had clock synchronization issues.
Audit Log Cleared	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows all events where an audit log was cleared from a host.
Audit Log Cleared per Attacker User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows the number of times an audit log was cleared by an attacker user name.
Audit Log Cleared per Attacker and Target	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows the number of times audit logs were cleared from a host by an attacker and target.

Audit Log Cleared per Target User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows the number of times an audit log was cleared by a target user name.
FISMA Reports Accessed	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query retrieves all the accessed FISMA reports ,who accessed those reports and when.
FISMA Reports Accessed by Report - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query retrieves all the FISMA report accessed eventsby specific report (default/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins)
FISMA Reports Accessed by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query retrieves all the FISMA reports accessedby specific user (default admin).
Information System Audit Tool Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query shows logins, both successes and failed, to information system audit tools.
Information System Audit Tool Logins by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query shows logins, both successes and failed, to information system audit tools for specific user (default admin).
All Actions per User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query lists all actions taken by a user.
All Administrator Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query lists all actions taken by an administrative user by ip address Administrative users are defined by the filter Administrative User.
All User Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query lists all actions taken by non-administrative user by ip address Administrative users are defined by the filter Administrative User.

Count of Failed Administrative Actions - Trend Query	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query counts the number of failed administrative actions per attacker user, target user and device product. Administrative users are defined in the filter Administrative User.
Failed Actions by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows failed action events by user (default admin).
Failed Administrative Actions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows failed administrative action events. Administrative users are defined by the filter Administrative User.
Failed Administrative Actions - Long Term	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows the trend of failed administrative actions over long term. This query can be run over a time period of up to 31 days. Administrative accounts are defined by the filter Administrative User.
Failed Administrative Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows failed administrative action events by IP address. Administrative users are defined by the filter Administrative User.
Failed User Actions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows failed non administrative action events. Administrative users are defined by the filter Administrative User.
Failed User Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows failed non administrative action events by IP address. Administrative users are defined by the filter Administrative User.
Logins and Logouts per User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query provides a listing of logins and logouts per user name.
Successful Actions by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows successful action events by user (default admin).
Successful Administrative Actions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows successful administrative action events. Administrative users are defined by the filter Administrative User.

Successful Administrative Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows successfuladministrative action events by IP address. Administrative users are defined by the filter Administrative User.
Successful User Actions by IP Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query shows successful non administrative action events by IP address. Administrative users are defined by the filter Administrative User.
All Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity flagged as information leakage.
Encrypted Communication Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows events which indicate a source is accessing sensitive information, although encrypted.
Former Employee Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity which involved former employees and flagged as information leakage.
Information Disclosure Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	Shows Information Disclosure vulnerabilities identified on the last 24 hours.
Monitored Accounts Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity which involved monitored accounts and flagged as information leakage.
New Hire Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity which involved new hire accounts and flagged as information leakage.
Organizational Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows events which indicate an organizational information leak.

Organizational Information Leaks on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows events which indicate an organizational information leak on network domain.
Personal Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows events which indicate a personal information leak.
Personal Information Leaks on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows events which indicate a personal information leak on network domain.
Privileged Accounts Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity which involved privileged accounts and flagged as information leakage.
Stale Accounts Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This query shows all activity which involved stale accounts and flagged as information leakage.
Configuration Changes - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Retrieves all configuration changes for the last hour and used as trend base query for the Configuration Changes trend.
Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made on the last 24 hours.
Configuration Modifications by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the changes were made to specific host name (default localhost).
Configuration Modifications by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows all configuration modifications by specific network domain (default operations).

Configuration Modifications by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows all configuration modifications by specific user (default admin).
Daily Trend - Configuration Changes by Address	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications by ip address.
Daily Trend - Configuration Changes by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications.
Daily Trend - Configuration Changes by User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications by user.
Database Configuration Modification	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows all events of database configuration modifications.
Firewall Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any firewall. Default time window: Last 24 hours.
Firewall Configuration Modifications by Firewall - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications by firewall host name (default localhost). Default time window: Last 24 hours.
Firewall Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications of any firewall.
Firewall Configuration Modifications by User - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any firewall by user (default admin). Default time window: Last 24 hours.

Network Device Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any network equipment.
Network Device Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications of network equipment.
Network IDS Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any network IDS. Default time window: Last 24 hours.
Network IDS Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications of network IDS.
Operating Systems Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made to operating systems.
Operating Systems Configuration Modifications by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made to operating systems on specific host name (default localhost).
Operating Systems Configuration Modifications by Process Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made to operating system specific process (default winlogon).
Operating Systems Configuration Modifications by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made to operating systems by specific user (default admin).
Top Firewalls with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top firewalls with most successful configuration modifications.

Top Network Devices with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top network devices with most successful configuration modifications.
Top Network IDS with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top network IDSs with most successful configuration modifications.
Top Users with Most Successful Firewall Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top users who made most successful configuration modifications.
Top Users with Most Successful Network Devices Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top users with most successful network devices configuration modifications.
Top Users with Most Successful Network IDSs Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top users with most successfulIDS configuration modifications.
Unsuccessful Operating Systems Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times unsuccessful changes attempted on operating systems.
Weekly Report - Configuration Modifications by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the changes were made to specific host name (default localhost) on the last 7 days.
Weekly Report - Configuration Modifications by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the changes were made to specific user name (default admin) on the last 7 days.
Weekly Trend - Configuration Changes by Address	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications by ip address.

Weekly Trend - Configuration Changes by Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications.
Weekly Trend - Configuration Changes by User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the top configuration modifications by user.
Account Change Details by Attacker User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts by specific attacker user (default admin).
Account Change Details by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts by specific host name (default localhost).
Account Change Details by Target User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts by specific target user name (default admin).
Account Change Details in Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts in specific network domain.
Code Signing Flaw Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Retrieves all the code signing flaw.
Successful Removal of Access Rights - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This query shows all the removal of access rights from a host resource in a particular domain.
Successful Removal of Access Rights by Target User Name Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This query shows all the removal of access rights by target user name (default admin).

New Systems by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems categorized under FIPS-199 or NIST800-53 by their network domains in the last month.
Number of New Systems by FIPS-199 Availability Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems under by FIPS-199 availability criticality level in the last month.
Number of New Systems by FIPS-199 Confidentiality Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems under by FIPS-199 Confidentiality criticality in the last month.
Number of New Systems by FIPS-199 Integrity Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems under by FIPS-199 Integrity criticality level.
Number of New Systems with FIPS-199 or NIST 800-53 High Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems categorized with high criticality under FIPS-199 or NIST 800-53 in the last month.
Number of New Systems with FIPS-199 or NIST 800-53 Low Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems categorized with low criticality under FIPS-199 or NIST 800-53 in the last month.
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems categorized with moderate criticality under FIPS-199 or NIST 800-53 in the last month.
Number of New Systems with FIPS-199 or NIST800-53 by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This query returns the number of new systems categorized under FIPS-199 or NIST800-53 by their network domains in the last month.
Asset Creation by Location	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of newly created assets.

Asset Deletion by Location	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of deleted assets.
Asset Identification Report	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows all assets and their respective network domain.
Asset Modification by Location	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of modified assets.
Assets by Application Type	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a list of all the assets for the environments. This query may (and should) be focused based on the environment of interest. Results are sorted by creation time.
Assets by Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a list of all the assets for the various network domains. This query may (and should) be focused based on the network domain of interest. Results are sorted by creation time.
Assets by Owner	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets listed by owners.
Assets without Assigned Owner	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets without owners.
Classification of Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows the asset classifications.
Critical Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.

Criticality of Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows the asset criticality.
Current Asset Count by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query provides the asset count for each network domain.
Current Asset Count by Network Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns the count of assets per network zone.
FIPS-199 Availability Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized with each FIPS-199 Availability Criticality.
FIPS-199 Confidentiality Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized with each FIPS-199 Confidentiality Criticality.
FIPS-199 Integrity Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized with each FIPS-199 Integrity Criticality.
Multi-homed Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns a list of multi-homed assets.
NIST 800-53 High Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized as NIST 800-53 high impact systems.
NIST 800-53 Low Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized as NIST 800-53 low impact systems.

NIST 800-53 Moderate Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query selects the total number of assets categorized as NIST 800-53 moderate impact systems.
Non-Operating System Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets which categorized as non OS Systems.
Operating System Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets which categorized as OS Systems.
Operating System Assets by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the OS assets by network domain.
Operating System Assets by Network Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides all the OS assets by network zone.
Operating System Assets by Operating System	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the distribution of OS assets by Operating system.
Software And Hosting Asset	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns the software detected along with information about the hosting assets.
Software Detected - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns events when a scanner detects a software product on a target host.
Software Products on Specific Asset	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns all software products detected on a specific asset in the last two weeks. The asset can be identified through either its address or host name.

Software Summary by Network Domain in Last 2 Weeks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns a summary of each software product (except operating systems) detected in the environment, grouped by network domain in the last two weeks.
Software Summary by Zone in Last 2 Weeks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns a summary of each software product (except operating systems) detected in the environment, grouped by zone in the last two weeks.
Software Summary in Last 2 Weeks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns a summary of each software product (except operating systems) detected in the environment in the last two weeks.
Top Hosts by Software Product in Last 2 Weeks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns the top ten hosts with most software products (except operating systems) detected in the environment in the last two weeks.
Top Zones by Software Product in Last 2 Weeks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query returns the top ten zones with most software products (except operating systems) detected in the environment in the last two weeks.
Assets Per Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query selects the total number of assets per criticality.
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query lists all the critical assets on network domain which have been categorized with a criticality of high or very-high. It can be used to identify key assets to implement the business continuity process.
Fault Logs on Critical Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query shows events indicating a process has failed to execute in the expected way on critical machine.
Information System Failures per Critical Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query shows the critical information system which generated error log entries.

Shutdown Machine not Started more than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query shows all shutdown machines which not started more than policy standard.
Shutdown of Critical Machines	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query shows all shutdown events of machines categorized as critical or highly critical.
Shutdown of Critical Machines on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query shows all shutdown events of machines categorized as critical or highly critical on network domain.
Weekly Trend - Shutdown of Critical Machines per Day	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query is based on trend "Shutdown of Critical Machines" and shows all weekly shutdown events of machines which categorized as critical.
Weekly Trend - Top 10 Shutdowns of Highly Critical Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query is based on trend "Shutdown of Critical Machines" and shows top 10 shutdowns of critical assets on the last week.
Zones Per Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query selects the total number of zones per criticality.
Identity Management Policy Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 1 Identification and Authentication Policy and Procedures/	Lists all the changes to identity management policies.
Identity Management Policy Violations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 1 Identification and Authentication Policy and Procedures/	Lists all the violations to identity management policy.
Count of Administrative Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows details of all successful administrative logins.

Count of Successful Administrative Logins in the Last 30 days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a count of successful administrative logins within the last 30 days.
Count of Unsuccessful Administrative Logins in the Last 30 days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a count of unsuccessful administrative logins within the last 30 days.
Daily Count of Successful User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retreives information about the number of successful non-administrative user logins every day over the past week.
Daily Count of Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Counts the number of unsuccessful daily user logins.
Default Vendor Account Involved on Information Leaks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows all activity which involved default vendor account and flagged as information leakage.
Default Vendor Account Involved on Internal Reconnaissance	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows all activity which involved default vendor account and flagged as internal reconnaissance.
Detail Default Vendor Account Used	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows if a vendor supplied user account without password is being used to login.

Non Multi Factor Access by Admin Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query retrieves events indicating a non multi factor authentication by admin accounts.
Number of Daily User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Captures the number of logins per on-administrative user and outcome over the entire day.
Number of Successful Administrative Logins by User and Host Information	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a listing of administrative users with successful logins grouped by user and host information. The administrative users are sorted by the number of attempts in a decreasing order.may (and should) be focused based on the Network Domain of interest.
Number of Unsuccessful Administrative Logins by User and Host Information	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Provides a listing of administrative users with unsuccessful login attempts, grouped by user and host information.The administrative users are sorted by the number of attempts in a decreasing order. This query may be focused based on the Network Domain of interest.
Replay Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retrieves events identifying replay attacks based on Microsoft event ID 4649.
Same User Using Different User Names	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query identifies users that have logged in using different user names.
Successful Administrative Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful administrative logins within the last day.

Successful Administrative Logins by Attacker Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful administrative logins within the last day by specific attacker host (default localhost)
Successful Administrative Logins by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retrieves the number of administrative successful user logins per hour.
Successful Administrative Logins by Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful administrative logins within the last day by specific target host (default localhost).
Successful Local Administrative Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful local administrative logins within the last day.
Successful User Local Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful local non-administrative user logins within the last day.
Successful User Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful non-administrative user logins within the last day.
Successful User Logins by Attacker Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successfulnon-administrative user logins within the last day by specific attacker host (default localhost)

Successful User Logins by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retrieves the number of non-administrative successful user logins per hour.
Successful User Logins by Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful non-administrative user logins within the last day by specific target host (default localhost)
Successful User Logins by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query shows details of all successful user logins within the last day by specific user (default admin)
Systems Accessed by Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows all systems that users have tried to access directly as default vendor account.
Top 10 Admin Users with Non Multi Factor Access	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query retrieves the top 10 admin users with non multi factor admin accesses.
Top 10 Assets with Non Multi Factor Admin Accesses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query retrieves the top 10 assets with non multi factor admin accesses.
Top Attackers Attempted Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top hosts from which attackers most attempted default vendor account.

Top Attackers Using Default Vendor Account	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top attackers successfully used a vendor supplied user account.
Top Attackers Using Direct Root or Administrator Account	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top attackers attempting direct root or administrator credential.
Top Default Vendor Accounts Attempted	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top vendor supplied user account still being used to login.
Top Default Vendor Accounts Used	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top vendor supplied user account still being used to login.
Top Target Hosts Where Default Vendor Account Attempted	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top hosts where a vendor supplied user account still being used to login.
Top Target Hosts Where Default Vendor Account Used	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top hosts where a vendor supplied user account still being used to login.
Top Target Hosts Where Direct Root or Administrator Account Observed	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the top hosts where direct root or administrator account is attempted.

Trend of Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the trend of unsuccessful administrative logins over long term.
Unsuccessful Administrative Logins - Long Term Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Counts the number of failed administrative logins per attacker user name, target user name and target address per month.
Unsuccessful Administrative Logins by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retrieves the number of administrative unsuccessful user logins per hour.
Unsuccessful User Logins by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Retrieves the number of non-administrative unsuccessful user logins per hour.
User Logged in from different IP Addresses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Selects single user names that have been used to login from different IP addresses.
Accepted Accesses Through AAA Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all the accepted accesses through AAA server.
All Critical Events in Last 24 Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all critical events related to DHCP servers in the last 24 hours.

All DHCP Leases by Particular Host Name in Last 24 Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all DHCP leases by a particular host name in the last 24 hours.
All DHCP Leases by Particular Offered IPv4 Address in Last 24 Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all DHCP leases by a particular offered IP address in the last 24 hours.
All DHCP Leases by Particular Offered IPv6 Address in Last 24 Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all DHCP leases by a particular offered IPv6 address in the last 24 hours.
All DHCP Leases by Particular Source MAC Address in Last 24 Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all DHCP leases by a particular MAC address in the last 24 hours.
DHCP Clients per Day in Last 7 Days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns the count of unique DHCP clients in the last seven days.
Lease Durations per Day in Last 7 Days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns the DHCP lease durations (rounded up to the hour unit) per day in the last seven days.
Leased IPv4 Addresses per Day in Last 7 Days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns the count of distinct leased IPv4 addresses in the last seven days.

Leased IPv6 Addresses per Day in Last 7 Days	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns the count of distinct leased IPv6 addresses in the last seven days.
Rejected Accesses Through AAA Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns all the rejected accesses through AAA server.
Unique MAC Count per Leased IP	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This query returns the count of unique MAC addresses leased to an IP.
All Password Change Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Provides a list of all password change events and their outcome.
All Password Change Events by User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Provides a list of all password change events and their outcome by specific user (default admin).
Failed Password Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Retrieves failed password change events, ordered by target user name.
Minimum Password Age Changed to Less than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This query retrieves events when minimum password age changed to Less than policy standard (default 60 days), you can change the default by editing referenced rule condition : "passwordAgedtoInt < 60" from 60 to different value which reflects your policy standard.
Minimum Password Length Changed to Less than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This query retrieves events when minimum password length changed to Less than policy standard (default 15 days), you can change the default by editing referenced rule condition : "minimumPasswordLength< 15" from 15 to different value which reflects your policy standard.

Password Policy Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This query retrieves all password policy changes based on windows events.
Password Spray Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Retrieves password spray attack on windows systems on the last day.
Passwords not Changed for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Lists accounts for which the password was not changed for longer than the policy standard permits.
Successful Password Changes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Lists successful password change events, ordered by target user name.
Unsecured Password Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Retrieves unsecured password events
Average Time to Resolution - By Case Severity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.
Average Time to Resolution - By Day	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows the average time to resolution of all the closed cases by day.This query should be run once a week and reported to management.
Average Time to Resolution - By User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows how long it takes individuals to close their cases. This query should be run once a week and reported to management.
Case Audit Events - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query collects Time to Resolution (TTR) information from case audit events and stores them in a trend for case history reporting.

Case Status by Owner	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query provides a breakdown by owner of all cases.
Cases by Stage	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query provides an overview of all cases in their current stages.
Open Cases	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows all currently open cases.
Open Cases by Control Families	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows all currently open cases by control family.
Open Cases by Control Family and Severity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows a breakdown of open cases by severity for each control family.
Open Cases by Owner	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows the number of open cases by owner.
Open Cases by Severity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query shows the number of open cases by severity.
Attacks Per 10 Minutes	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves attacks number per 10 minutes on the last hour.
Attacks and Suspicious Activities - Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query summarizes the attakcs and suspicious activities for the last hour.
Attacks and Suspicious Activities From a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events coming from a particular network domain sorted by the event's end time.

Attacks and Suspicious Activities Targeting a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events targeting a particular network domain sorted by the event's end time.
Attacks and Suspicious Activities by Attacker Address - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by attacker address.
Attacks and Suspicious Activities by Attacker Zone - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by attacker zone.
Attacks and Suspicious Activities by Country	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by country.
Attacks and Suspicious Activities by Target Host - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by target host.
Attacks and Suspicious Activities by Target Port - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by target port.
Attacks and Suspicious Activities by Target Zone - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events by target zone.
Attacks and Suspicious Activities from specific Country - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events from specific country (country code should be provided on lower case,default us).
Count of Attacks and Suspicious Activities Per Attacker Machine	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a count of attacker addresses appearing in of hostile or suspicious events.

Count of Attacks and Suspicious Activities Per Target Machine	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a count of target addresses appearing in of hostile or suspicious events.
Daily Report - Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events.
High Priority Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query shows events in which the Priority is 10.
Internal Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events from internal attacker targeting internal assets.
Internal Reconnaissance Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all internal reconnaissance events.
Internal Reconnaissance Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query shows the top events executed for internal reconnaissance.
Internal Reconnaissance Sources	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query shows the sources conducting internal reconnaissance.
Internal Reconnaissance Targets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query shows the targets accessed by internal reconnaissance activity.
Reconnaissance Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all reconnaissance events.
Reconnaissance Activities From a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all reconnaissance activities events coming from a particular network domain sorted by the event's end time.
Reconnaissance Activities Targeting a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all reconnaissance activities events targeting a particular network domain sorted by the event's end time.

Reconnaissance Activities from specific Country - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all reconnaissance activities events from specific country (country code should be provided on lower case,default us).
Top 5 Attacker Countries	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top 5 attacker countries on the last hour.
Top 5 Attackers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top 5 attacker addresses on the last hour.
Top 5 Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top 5 attacks on the last hour.
Top 5 Targets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top target hosts on the last hour.
Weekly Report - Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query provides a listing of all hostile or suspicious events on the last 7 days.
Weekly Trend - Attacks Per Day	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves attacks number per day.
Weekly Trend - Top 5 Attackers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top attackers on the last week.
Weekly Trend - Top 5 Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top attacks on the last week.
Weekly Trend - Top 5 Targets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query retrieves the top targets on the last week.

Critical Machine Configuration Modifications at Unscheduled Time	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	Shows the number of times changes were made to critical machines on unscheduled time.
Network Device Configuration Modifications at Unscheduled Time	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	Shows any unscheduled configuration modifications of any network equipment.
System Shutdown or Restart at Unscheduled Time	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This query shows unscheduled shutdown or restrart of hosts in the last 24 hours.
Unscheduled Change in Status of Service	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This query shows the starting or stopping of services outside of scheduled maintenance windows.
All Actions by User at Maintenance Time - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 3 Maintenance Tools/	This query lists all actions taken by a specific user at maintenance time.
Failures at Maintenance Time by Target Host - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 3 Maintenance Tools/	This query retrieves the number of information failures at maintenance time by target host name.
All Specific Host Actions which Originated from Remote at Maintenance Time - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 4 Nonlocal Maintenance/	This query lists all actions taken on specific host from remote at maintenance time.
Removable Media Accesses After Work Hours	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	Shows all the removable media accesses after work hours.
Successful Logins to Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This query retrieves a listing of successful login attempts to specific network domain.
Unsuccessful Logins to Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This query retrieves a listing of unsuccessful login attempts to specific network domain.

Removable Media Activity Plugged In Multiple Assets in Short Period of Time	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	This query retrieves removable media plugged In multiple assets in short period of time.
After Hours Successful Monitored Accounts Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Shows details of all after hours successful monitored accounts logins within the last day.
All Successful Actions by Monitored Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This query lists all successful actions taken by monitored accounts.
Monitored Accounts Email Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This query retrieves all email activity by monitored accounts.
New Hires Email Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This query retrieves all email activity by new hires.
Suspicious Activity by Monitored Accounts	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all the identified suspicious activity performed by monitored accounts on the last 24 hours.
Unsuccessful Monitored Accounts Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Shows details of all failed monitored accounts logins within the last day.
List of Terminated Employees on the last Day	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 4 Personnel Termination/	This query retrieves all terminated employees on the last day.
Building Access and Leave by Building	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by bulding.
Building Access and Leave by Contractors	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by contractors.

Building Access and Leave by User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by user.
Building Access and Leave by Visitors	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by visitors.
Failed After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows failed attempts to leave a building at any time.
Successful After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Successful Building Access Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access events at all times.
Successful Building Access Granting	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows all successful building access granting.
Successful Building Leaving Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows all successful building leaving events at all times (for badge reader systems support this option).
Machines Conducting Policy Breaches	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows machines which were involved in policy breaches.

Machines Conducting Policy Violations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows machines which were involved in policy violations.
Top 20 Policy Breach Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 20 policy breach events.
Top 20 Policy Violation Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 20 policy Violation events.
After Hours Successful New Hire Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows details of all after hours successful new hire logins within the last day.
All Events by New Hires	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query shows all events by new hires.
Email Activity by User	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query retrieves the emails sent by specific user.
Former Employee Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified outbound internet activity of former employees. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Monitored Accounts Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified outbound internet activity of monitored employees. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
New Hire Account Added to Groups	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows all new hire accounts added to groups.
New Hire Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified outbound internet activity of new hire users. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Non Privileged Accounts Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified outbound internet activity of non privileged accounts. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.

Privileged Accounts Internet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified outbound internet activity of privileged accounts. Internet activity is defined as a successful connection to external addresses on ports 80, 443, 21 or 20.
Summary of Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query displays the number of suspicious events per new hire.
Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified suspicious activity performed by new users.
Top Email Receivers by Email Size	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query shows the top email recipients based on the size of emails received.
Top Email Receivers by Number of Emails	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query shows the top email recipients based on the number of emails received.
Top Email Senders by Email Size	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query shows the top email senders based on the size of emails sent.
Top Email Senders by Number of Emails	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This query shows the top email senders based on the number of emails sent.
Unsuccessful New Hire Logins	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows details of all unsuccessful user logins within the last day.
Severe Information Disclosure Vulnerabilities on PII Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Shows severe information disclosure vulnerabilities on PII assets identified on the last 24 hours.
Targeted Recon Activity from the Same Country against Multiple PII Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This query shows all activity flagged as targeted Recon activity from the same country against multiple PII Assets.

Unauthorized Access of Information on PII Asset	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This query shows all activity flagged as unauthorized access of information on PII assets.
Unsuccessful Logins by the Same User to Multiple PII Assets on Short Period	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This query shows all activity flagged as unsuccessful logins by the same user to multiple PII assets on short period.
Assets with E-Authentication Levels	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	This query returns all the assets withE-Authentication levels in the environment.
Count Assets per E-Authentication Level 3 or 4	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	This query returns the count of assets with each E-Authentication level in the environment.
Count of Assets with E-Authentication Level 3 or 4 per Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	This query returns the number of assets with E-Authentication Level 3 or 4 per zone.
Insider Threat	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	Retrieves critical attacks launched by multiple internal attackers against the same network domain using the same pattern of attack.
Malicious Code Activities from Internal Sources	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	Shows all malicious code activities from internal sources.
Top Internal Sources with Malicious Code Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	Shows the top internal sources with most malicious code activities.

Shared Machines among Test Environment and Personal Identifiable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	Returns all assets that are shared between Test environment and Personal Identifiable assets.
CVSS Score Greater than or Equal to 8	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows vulnerabilities with CVSS >=8.
CVSS Score Greater than or Equal to 8 on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows vulnerabilities with CVSS >=8 on the last 7 days.
List of Vulnerability Scanners not run for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	This query retrieves vulnerability scanners which not run for longer than policy standard.
Missing Security Patches Summary	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of the missing security patches summary.
Overflow Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows overflow vulnerabilities identified on the last 24 hours.
Overflow Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the overflow vulnerabilities for the last 7 days.
SQL Injection Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows SQL injection vulnerabilities identified on the last 24 hours.
SQL Injection Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the SQL injection vulnerabilities for the last 7 days.
Top 10 Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerabilities on FISMA Assets.

Top 10 Vulnerable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerable FISMA assets.
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerable Assets by network domain (default Development)
Top Critical Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves the top 20 critical vulnerabilities for the last 14 days.
Top Vulnerable IP Addresses	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves the top 10 vulnerable IP Addresses for the last 14 days.
Vulnerabilities - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last hour. Used as trend base query for the vulnerabilities trend.
Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last 14 days.
Vulnerabilities Summary	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of the vulnerability summary on the organization.
Vulnerabilities Summary - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of the vulnerability summary on the organization on the last 7 days.
Vulnerabilities Summary on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of the vulnerability summary on specific network domain (default Development) on the last day.
Vulnerabilities by CVE ID	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last day for specific CVE ID.

Vulnerabilities by CVE ID - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last 7 days for specific CVE Id.
Vulnerabilities by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last day for specific Host Name.
Vulnerabilities by Host Name - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the vulnerabilities for the last 7 days for specific Host Name.
Vulnerability Events By Scanner - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows vulnerability count per scanner for the last 14 days.
Vulnerability Scans - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows all the vulnerability scans for the last 14 days
XSRF Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows XSRF vulnerabilities identified on the last 24 hours.
XSRF Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the XSRF vulnerabilities for the last 7 days.
XSS Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows XSS vulnerabilities identified on the last 24 hours.
XSS Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Retrieves all the XSS vulnerabilities for the last 7 days.
Count of DoS Attacks per Day	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query counts the total number of weekly denial of service attack events.

Count of DoS Attacks per Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query counts the total number of daily denial of service attack events.
DoS Attacks Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query summarizes the number of DoS attacks for long term reporting.
DoS Attacks by Attacker	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query provides a weekly count of attacker addresses appearing in DoS attack events.
DoS Attacks by Target	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query provides a weekly count of target addresses appearing in DoS attack events.
Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows the details of successful denial of service attacks.
Target Object in Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows the number of times a particular object has been a victim of denial of service attacks.
Target Object in Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows the number of times a particular object has been attempted to be attacked by denial of service attacks.
Top DoS Attackers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows the top attackers responsible for initiating denial of service attacks.
Top DoS Targets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows hosts which were targeted the most with denial of service attacks.

Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This query shows the details of unsuccessful and attempted denial of service attacks.
Blocked Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Blocked Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query provides a listing of the outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query provides a listing of the iinbound firewall traffic directed at assets in the indicated Network Domain of interest.
Open Firewall Port Details	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query gives details of all the ports that are allowed to pass through various firewalls.
Organizational Information Leaks Originated from Third Party	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query shows events which indicate an organizational information leak originated from third-party assets.
Personal Information Leaks Originated from Third Party	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query shows events which indicate a personal information leak originated from third-party assets.
Policy Violations Originated from Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	Provides a listing of events categorized by ArcSight as policy violations which originated from various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.

Policy Violations on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.
Reconnaissance from Third Party Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query shows reconnaissance activity from assets in the Remote domain.
Third-Party Incidents - Closed Cases	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query shows all cases involving third-party systems that have been closed.
Third-Party Incidents - Open Cases	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This query shows all cases involving third-party systems that are still open.
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	Shows the top 10 vulnerable Assets by network domain (default Development)
Internal Insecure Service Providers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Returns the internal providers of insecure services.
Internal Insecure Transmissions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all internal traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Outbound Insecure Transmissions	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all outbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.

Traffic Anomaly on Application Layer	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This query shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This query shows traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This query shows traffic anomaly on transport layer.
Unencrypted Services by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Returns all unencrypted services by a particular host name identified in the last 24 hours using vulnerability and port scanning events.
Cryptographic Hash Algorithm Related Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the cryptographic hash algorithm related vulnerabilities for the last 7 days.
Cryptographic Hash Algorithm Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Cryptographic Public Key Related Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the cryptographic public key algorithm related vulnerabilities for the last 7 days.
Cryptographic Public Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential public key related vulnerability was detected.

Cryptographic Symmetric Key Related Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the cryptographic symmetric algorithm related vulnerabilities for the last 7 days.
Cryptographic Symmetric Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Related Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the cryptographic weak protocol algorithm related vulnerabilities for the last 7 days.
Cryptographic Weak Protocol Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
SSH Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that SSH vulnerability has been detected.
SSH Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the SSHvulnerabilities for the last 7 days.
SSL|TLS Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that SSL/TLS vulnerability has been detected.
SSL|TLS Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all SSL/TLS vulnerabilities for the last 7 days.
VPN Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Selects events indicating that VPN vulnerability has been detected.

VPN Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Retrieves all the vpn vulnerabilities for the last 7 days.
Invalid or Expired Certificate	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Shows incidents which indicate that an invalid or expired certificate was detected.
Mobile Code Detection	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-18 Mobile Code/	This query retrieves mobile code detected by Nessus or Snort products.
VOIP Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This query provides a listing of all VOIP hostile or suspicious events.
VOIP Traffic Anomaly	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This query shows traffic anomaly related to VOIP applications.
VOIP Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Shows voice over ip vulnerabilities identified on the last 24 hours.
VOIP Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Retrieves voice over ip vulnerabilities for the last 7 days.
DNS Queries	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrives DNS queries on the last day.

DNS Queries by Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrives DNS queries by queried domain on the last day.
DNS Queries by Originator	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrieves DNS queries by originator on the last day.
Weird DN Queries	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrives DNS queries by hour.
Weird DN Queries by Attacker	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrives DNS queries by hour.
Weird DN Queries by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	Retrives DNS queries by hour.
Information Interception Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This query shows information interception activity.
Redirection Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This query shows redirection attacks.

Honeypot Interaction Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This query shows all honeypots events received last 24 hours.
Insecure Cryptographic Storage	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Selects events indicating that insecure cryptographic storage has been detected.
Insecure Cryptographic Storage - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Retrieves all the XSRF vulnerabilities for the last 7 days.
Covert Channel Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-31 Covert Channel Analysis/	This query shows all covert channel activity.
Meltdown|Spectre Vulnerability Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	This query retrieves Meltdown|Spectre related flaws reported by vulnerability scanners.
Anti-Virus Stopped or Paused	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all events when a anti-virus service is stopped or paused in the last day.
Anti-Virus Stopped or Paused - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all events when a anti-virus service is stopped or paused in the last week.
Daily Anti-Virus Stopped or Paused - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all events when a anti-virus service is stopped or paused on systems.
Failed Anti-Virus Updates	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all the failed Anti-Virus updates on systems.

Failed Virus Removal Events	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows all the failed virus removal events.
Hacker Tools Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows hacker tools activity against the organization.
Shellcode Execution Detected	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows shellCode execution events.
Top Hosts with Most Spyware Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Finds the top 10 systems with most spyware activities (routine maintenance and remediation events).
Top Hosts with Most Virus Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows the top hosts with most virus activities detected on systems.
Top Spyware Instances	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Provides the names of the top 10 detected spyware instances.
Top Virus Instances	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of virus activities detected on systems sorted by virus.
Top Zones with Most Virus Activities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows the top zones with most virus activities detected on systems.
Trojan Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows all trojan activity on the last 24 hours.

Virus Activity by Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows virus activity by hour.
Virus Activity by Target Host	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows virus activity by target host.
Virus Activity by Virus Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows virus activity by target host.
Worm Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows all worm activity on the last 24 hours.
Email Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query shows all email attacks.
Email Traffic with Competitors	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query retrieves emails with competitors.
Installed Windows Systems by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query lists all the installed windows systems events by specific host (default localhost) on the last 24 hours.
Phishing Attacks	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query shows all email attacks.
Possible Botnet Activity	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query shows possible C&C activity.

Top Phishing Email Receivers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query shows the top phishing email recipients.
Top Phishing Email Senders	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query shows the topPhishing email senders.
User Logged in from Two Countries	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This query selects user names that have been used to login from two different countries.
BIOS Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Shows BIOS vulnerabilities identified on the last 24 hours.
BIOS Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Retrieves all the BIOS vulnerabilities for the last 7 days.
File Creations by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all created files detected based on reports from the File Integrity Checker on specific host name (default localhost) . Default time window: Last 24 hours.
File Creations by Host Name per Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all created files detected based on reports from the File Integrity Checker on specific host name (default localhost) by hour. Default time window: Last 24 hours.
File Deletions by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all deleted files detected based on reports from the File Integrity Checker on specific host name (default localhost) . Default time window: Last 24 hours.

File Deletions by Host Name per Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all deleted files based on reports from the File Integrity Checker on specific host name (default localhost) by hour. Default time window: Last 24 hours.
File Integrity Changes by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all file changes detected based on reports from the File Integrity Checker on specific host name (default localhost) . Default time window: Last 24 hours.
File Integrity Changes by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all file changes detected based on reports from the File Integrity Checker on specific domain (default development) . Default time window: Last 24 hours.
Integrity Tools	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query detects integrity tools reporting to ArcSight ESM based on ArcSight Categorizations. Default time window: Last 24 hours.
Software Changes by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all changes to any software installed on specific host (default localhost).
Software Changes by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This query shows all changes to any software installed on specific domain (default development).
Spam per Hour	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This query gets the number of spam emails sent every hour over the past day.
Top Spam Receivers	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This query shows the top phishing email recipients.

Top Spam Senders	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This query shows the topPhishing email senders.
Command Injection on HTTP Request	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	Shows command injection on HTTP requests.
ASLR or Data Execution Prevention Bypass Flaws	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Shows an ASLR or Data Execution Prevention Bypass Flaws on the last 24 hours.
ASLR or Data Execution Prevention Bypass Flaws - on Trend	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Shows an ASLR or Data Execution Prevention Bypass Flaws on the last 7 days.
Disabled Data Execution Prevention (DEP) Mechanism	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	This query retrieves events on the last 24 hours indicating that a data execution prevention is disabled , is based on Nessus signature id 24282.
Attempted File Changes in Development originated from Other Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Displays attempts to change a file on a host in the development segment from a source that is in a specific network domain. By default, the Production network domain is used. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
File Changes in Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This query counts the number of creations, deletions and modifications of files on systems in the development network domain.
Successful Administrative Logins to Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This query identifies successful logins with an administrative account to development systems.

Successful User Logins to Development Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This query retrieves successful logins using a non-administrative account, to assets categorized as Development.
Unsuccessful Administrative Logins to Development Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This query retrieves failed logins using an administrative account, to assets categorized as Development.
Unsuccessful User Logins to Development Systems	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This query retrieves failed logins with a non-administrator account to assets categorized as Development.
New Development Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	This query retrieves all the new development vulnerabilities that identified on the last scan.
Non Fixed Development Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	This query retrieves all the persistent development vulnerabilities that identified on reoccurring scans and not fixed by developers.
Former Employee Accounts in Use	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies all former employee user names and reporting device details associated with recent events.
Account Lockouts	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows all account lockout events in the last hour. You can drill down on either the host address or the user name for more focused results.
Frequent Unsuccessful Logins by User Name	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query viewer displays all user names for which there are a continuous set of unsuccessful login attempts.

Frequent Unsuccessful Logins from Attacker Host	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query displays all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.
Frequent Unsuccessful Logins to Target Host	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This query viewer lists all target hosts which have received a continuous set of unsuccessful login attempts.
Logging Devices	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 6 Audit Review, Analysis, and Reporting/	This query viewer shows the different products that are logging to ArcSight ESM.
Failed Administrative Actions in the Last Hour	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query viewer shows failed administrative actions in the last hour. Administrative users are defined by the filter Administrative User.
Failed User Actions in the Last Hour	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query viewer shows failed non administrative actions in the last hour. Administrative users are defined by the filter Administrative User.
Successful Administrative Actions in the Last Hour	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This query viewer shows successful administrative actions in the last hour. Administrative users are defined by the filter Administrative User.
Asset Count per Network Domain	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the asset count for each business network domain.
FIPS-199 Availability Criticality Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the total number of assets categorized with each FIPS-199 Availability Criticality.
FIPS-199 Confidentiality Criticality Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the total number of assets categorized with each FIPS-199 Confidentiality Criticality.

FIPS-199 Integrity Criticality Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the total number of assets categorized with each FIPS-199 Integrity Criticality.
Multi-homed Assets	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer lists all multi-homed assets.
NIST 800-53 High Impact Assets Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer selects the total number of assets categorized as NIST 800-53 high impact systems.
NIST 800-53 Low Impact Assets Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer selects the total number of assets categorized as NIST 800-53 lowimpact systems.
NIST 800-53 Moderate Impact Assets Overview	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer selects the total number of assets categorized as NIST 800-53 moderate impact systems.
Operating System Assets by Network Domain	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows all the OS assets by network domain.
Operating System Assets by Network Zone	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows all the OS assets by network zone.
Operating System Assets by Operating System	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows all the OS assets by operating system.
Top 10 Software Products	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the top 10 software products detected on most assets.

Top Hosts with Most Software Products	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewerreturns the top ten hosts with most software products (except operating systems) detected in the environment in the last two weeks.
Top Zones with Most Assets	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the top ten zones with the most assets.
Top Zones with Most Software Products	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This query viewer shows the top ten zones with the greatest number of software products (except operating systems) detected in the environment in the last two weeks.
Assets Per Criticality	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query viewer selects the total number of assets per criticality.
Zones Per Criticality	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This query viewer selects the total number of zones per criticality.
Assets with Non Multi Factor Admin Accesses	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This Query Viewer shows the number of Non Multi Factor Admin Accesses per asset.
Count of Successful Administrative Logins in the Last 30 Days	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a count of unsuccessful administrative logins in the last 30 days, ordered by the most occurring failures.
Count of Unsuccessful Administrative Logins in the Last 30 Days	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows a count of unsuccessful administrative logins in the last 30 days, ordered by the most occurring failures.

Top 10 Admin Users with Non Multi Factor Accesses	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This query viewer displays the top 10 Admin Users with Non Multi Factor Accesses.
Password Changes	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Shows all password change events.
Open Cases	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query viewer shows all open cases.
Open Cases by Control Family	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query viewer shows the number of open cases by control family.
Open Cases by Owner	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query viewer shows the number of open cases by owner.
Open Cases by Severity	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This query viewer shows the number of open cases by severity.
Attacks Per 10 Minutes	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer shows reported attacksper 10 minutes interval.
Attacks and Suspicious Activities	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer summarizes the attacks and suspicious activities for the last hour and used as drill down mechanism through the dashboard "Attacks and Suspicious Activities “ Investigation" .
Top 5 Attacker Countries	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer shows the top 5 attacker countries on the last hour.
Top 5 Attacks	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer shows the top 5 attacks on the last hour.

Top Attackers	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer shows the top attackers on the last hour.
Top Targets	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This query viewer shows the top targets on the last hour.
All Events by New Hires	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows all events by new hires.
Suspicious Activities by New Hires	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Shows all suspicious activities by new hires.
Top Critical Vulnerabilities	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows summary of top critical vulnerabilities,where the user can drill down to detailed information about those vulnerabilities.
Top Vulnerable IP Addresses	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows top vulnerable IP addresses in bar chart format, the user can drill down to all vulnerabilities by IP Address.
Vulnerabilities	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows all the vulnerabilities.
Vulnerability Events By Scanner	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows vulnerability events count for each scanner.
Vulnerability Scans	QueryViewer	/All Query Viewers/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows all the vulnerability scans for the last 14 days, where the user can drill down to all the vulnerabilities which pertains to specific scan.
Account Creations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This reports shows all account creations.

Account Creations in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were created in a specific network domain. The network domain has to be specified at report runtime (default Development). Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Deletions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	This reports shows all account deletions.
Account Deletions in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were deleted in a specific network domain (default Development). The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Account Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all account modifications.
Account Modifications by Attacker User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were modified by specific user (default admin). The user has to be specified at report runtime.
Account Modifications by Target User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of all the modification of a specific information system account (default admin).The user has to be specified at report runtime.
Account Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Provides a listing of Information System accounts that were modified in a specific network domain (default Development). The network domain has to be specified at report runtime. Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Activity by Former Employees	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows any activity performed by users who are known to be terminated.

Disabled Privilege User Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all disabled privilege user accounts.
Disabled User Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all disabled user accounts.
Enabled User Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all enabled user accounts.
Failed or Attempted Removal of Access Rights	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all the attempts or failed removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
Former Employee Account Access Attempt	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists all login activity from any former employee.
Inactive User Account Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user names that are in the Stale Accounts active list.
Login Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows login activity by users that are on the Stale Accounts Active List. The report is ordered by the outcome of the login event.
Privileged Account Change Details	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists details of events when an Privileged account was attempted to be changed
Successful Removal of Access Rights	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows the removal of access rights from a host resource.
Suspicious Activities by Former Employee	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Lists all suspicious activities by any former employee.

Suspicious Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows suspicious activity by users that are on the Stale Accounts Active List.
User Group Account Creations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user group creations.
User Group Account Deletions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user group deletions.
User Group Account Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user group modification.
Users Added or Removed from Group - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user accounts which added or removed from specific groups.
Users Added to Groups	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all user accounts added to groups.
Users Removed from Groups	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Shows all users accounts removed from groups.
Login Activity from Non Classified Machines to Classified Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Shows all login activity from non classified machines to classified machines.
Login Activity to Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Shows all login activity to critical machines.
Unauthorized Access to High Impact Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	Shows all unauthorized accesses to high impact systems. This report requires the following rule "Unauthorized Access to High Impact Systems" to be enabled and deployed.

Access to Network Domains from Machines not in that Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows all successful access attempts to systems in a particular Network Domain from systems not in that domain. the network domain has to be specified at report runtime (default Development) exactly as it mentioned under /All Asset Categories/ArcSight Solution/Network Domains. This report is a template and you could create focused reports based on it.
Attacks from Non Classified Machines to Classified Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all attacks from non classified machines to classified machines.
Cross-Talk Between Network Domains - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows all cross-talk in the last 24 hours between assets in 2 network domains . default network domains : development and test.
High to Low Classified Asset Communication	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.
High to Low Classified Traffic Information Leak	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all information leaks from classified machines to non-classified machines.
Low to High Classified Asset Communication	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.
Suspicious Activity on Network Domains from Machines not in that Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows all attacks and suspicious activity to systems in a particular Network Domain from systems not in that domain. the network domain has to be specified at report runtime (default Development) exactly as it mentioned under /All Asset Categories/ArcSight Solution/Network Domains. This report is a template and you could create focused reports based on it.
Traffic Between Zones	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows the target ports between zones.

Traffic Coming from Dark Address Space	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic from Classified Machines to Non Classified Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all traffic from classified machines to non classified machines.
Traffic from Non Classified Machines to Classified Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Shows all traffic from non classified machines to classified machines.
Traffic to Dark Address Space	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This report shows all traffic directed to a dark address range. This should be considered very suspicious.
Attacks from Development Targeting Production	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides a listing of hostile or suspicious traffic from development machines targeting production facilities.
Attacks from Production Targeting Development	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Provides a listing of hostile or suspicious traffic from production facilities targeting development machines.
Development and Test Cross-Talk	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Shows all cross-talk in the last 24 hours between assets in Development category and assets in Test category.
Multiple Functions Implemented on a Server	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Returns all assets that implement multiple functionality, for example, a database and Web server installed on the same machine.
Operations and Development Cross-Talk	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Shows all cross-talk in the last 24 hours between assets in Operations category and assets in Development category.
Shared Machines among Test, Development and Operations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Returns all assets that are shared between at least two of the Test, Development, and Operation domains.

Test and Development Accounts in Production Environment	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This report shows test and development accounts which used in production environment. Please make sure the following rule "Test and Development Accounts in Production Environment" is enabled and deployed before you run this report.
Test and Operations Cross-Talk	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Shows all cross-talk in the last 24 hours between assets in Test category and assets in Operations category.
Special privileges assigned to new logon	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 6 Least Privilege/	Shows events which identifies when a special privileges assigned to new logon.
Account Lockouts per System	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows a count of account lockouts per system. It also shows the number of distinct user names that contributed to the total number of lockouts.
Account Lockouts per User and System	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows a counts of account lockouts per user and system, and a chart of the total number of lockouts per user.
Application Brute Force Login Attempts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Displays all user names for which there are a continuous set of unsuccessful login attempts.
Frequent Unsuccessful Logins from Attacker Host	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Displays all attacker hosts from which a continuous set of unsuccessful login attempts have been occurring.
Frequent Unsuccessful Logins to Target Host	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Lists all target hosts which have received a continuous set of unsuccessful login attempts.
Successful Brute Force Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Provides a listing of events categorized by ArcSight as probable successful brute force login attempts.may (and should) be focused based on the Network Domain of interest.

Unsuccessful User Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This report provides a listing of unsuccessful user login attempts.
Unsuccessful User Logins by Attacker Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This report provides a listing of unsuccessful user login attempts by specific attacker host (default localhost).
Unsuccessful User Logins by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This report provides a listing of unsuccessful user login attempts by target host (default localhost).
Unsuccessful User Logins by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This report provides a listing of unsuccessful user login attempts by User(default admin).
Workstation Locked\Unlocked Events by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Shows all information about workstation locks by specific user, it's based on windows events, the user has to be specified at report runtime in lowercase (default admin).
Workstation Locked\Unlocked Events by Workstation - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Shows all information about workstation locks by workstation, it's based on windows events, the workstation has to be specified at report runtime in lowercase (default localhost).
Workstation Locked\Unlocked Events by Workstation and User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-11 Device Lock/	Shows all information about workstation locks by workstation and user name, it's based on windows events, the workstation and user has to be specified at report runtime in lowercase (default localhost and admin).
RDP Session is not Terminated for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	This report shows RDP Sessions which was not changed for longer than the policy standard permits.
Bypassing Authentication or Authorization Flaw Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification or Authentication/	Displays all the bypassing authentication or authorization flaws Detected.

Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification or Authentication/	Displays all the identified internet activity performed by users.
Internet Activity by Attacker Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification or Authentication/	Displays all the identified outbound internet activity by specific attacker address (default 127.0.0.1) .
Internet Activity by Target Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification or Authentication/	Displays all the identified outbound internet activity by specific target address (default 127.0.0.1) .
Internet Activity by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification or Authentication/	Displays all the identified outbound internet activity by specific user (default admin) .
All VPN Access Attempts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all VPN access attempts.
Attacks and Suspicious Activities from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows all hostile or suspicious events from Remote assets sorted by the event's end time.
Detail Disallowed Port Access	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows traffic that should not be seen per the Allowed Ports/Disallowed Ports active list.
Disallowed Port Access Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows several summary aspects of traffic to disallowed ports.
Disallowed Port Attempted or Failed Access Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows attempts or failed access to disallowed ports.
Inbound Insecure Transmissions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.

Inbound Traffic	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report provides a count of inbound traffic.
List of VPN Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows any configuration modifications of any vpn device.
Organizational Records Information Leaks Originated from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows the communications which were classified as information leaks of organizational records originated from Business Associate domain.
Personal Information Leaks Originated from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows events which indicate a personal information leak originated from remote systems.
Privileged VPN Remote Access Attempts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows remote VPN connections attempts by an administrative account. The report is ordered by the connection outcome so you can easily distinguish the successful connections from the unsuccessful ones.
Reconnaissance from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report shows reconnaissance activity from remote systems.
Successful Administrative Logins from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report displays all successful administrative logins from assets categorized as Remote.
Successful Non VPN Remote Accesses	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Lists all non VPN remote accesses/
Successful User Logins from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report displays all successful non-administrative logins from assets categorized as Remote.
Successful VPN Access by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report provides all successful VPN accesses by specific user ,The user has to be specified at report runtime (default admin).

Suspicious Activities to Disallowed Ports Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows suspicius traffic that should not be seen per the Allowed Ports active list.
Unsuccessful Administrative Logins from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report displays all failed logins with an administrative account from assets categorized as Remote.
Unsuccessful User Logins from Remote Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	This report displays all failed logins with a non-administrative account from assets categorized as Remote.
Unsuccessful VPN Access	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Provides a listing of failed VPN access, the number of such failed events and the last failure time.
VPN Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Shows vpn modifications summary.
Bluetooth Protocol Vulnerability Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This report displays Bluetooth protocol related flaws reported by vulnerability scanners.
Count of Attacks and Suspicious Activity Event Names in the Wireless Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	Displays a count of the event names of attack and suspicious activity events in the Wireless Network Domain sorted by the most common events. It also displays the number of unique target machines that were affected by the event. Note: For events to appear in this report either the attacker or target zones or assets need to be categorized in the Wireless asset category.
Wireless Encryption Violations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	Shows all wireless encryption violations.
Wireless Malicious Traffic Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This report shows all incidents when wireless malicious traffic is detected.
Wireless Security Protocol Vulnerability Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This report displays flaws reported by vulnerability scanners which related to wireless security protocols such as WEP,WPA,WPA2 etc..

Disallowed Port Attempted or Failed Access Summary from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report shows attempts or failed access to disallowed ports.
Disallowed Port Successful Access Summary from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report shows successful access to disallowed ports.
Removable Media Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours using windows events.
Removable Media Activity by Device- Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours using windows events by device (The file name/device object has to be specified at report runtime).
Removable Media Activity by Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours using windows events by hostname (default localhost).
Removable Media Activity by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Shows all the removable media activity for the last 24 hours using windows events by user (default admin).
Successful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all successful administrative logins from assets categorized as Third Party.
Successful Administrative Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all successful logins to assets categorized as Third Party, that were done with an administrator account.
Successful User Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all successful non-administrative logins from assets categorized as Third Party.
Successful User Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all successful non-administrative logins to assets categorized as Third Party.

Third-Party Access	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report shows all access attempts to assets by third parties.
Unsuccessful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all failed logins with an administrative account from assets categorized as Third Party.
Unsuccessful Administrative Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all failed logins with an administrative account to assets categorized as Third Party.
Unsuccessful User Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all failed logins with a non-administrative account from assets categorized as Third Party.
Unsuccessful User Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	This report displays all failed logins with a non-administrative account to assets categorized as Third Party.
Possible Bitcoin Mining Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-23 Data Mining Protection/	This report displays possible bitcoin mining machines, by default it based on Nessus vulnerability scanner plugin "56195",you can customize its referenced filter to include additional signatures. Before running this report make sure the following rule "Possible Bitcoin Mining Activity" is enabled and deployed.
Assets that Failed Technical Compliance Check	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	This report shows assets which failed the technical compliance check.
Attacks and Suspicious Activities Targeting Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows all hostile or suspicious events targeting third party domain sorted by the event's end time.
Attacks and Suspicious Activities from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows all hostile or suspicious events from Third Party domainsorted by the event's end time.

Communication between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows communications between assets in 2 network domains . default network domains : development and test.
External to Internal Traffic	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report provides a count of inbound traffic.
Internal to External Traffic	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report provides a count of outbound traffic.
Successful Administrative Logins between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This report shows successful administrative logins with an administrator account between assets in 2 network domains . default network domains : development and test.
Information System Failures	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This report shows all information system failure events.
Penetration Testing not Performed for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 8 Penetration Testing/	This query displays assets which penetration testing not Performed for themlonger than policy standard.
Windows Domain Policy Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Displays changes to Microsoft Domain Policy for the last 24 hours.
Windows Group Policy Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Displays changes to Microsoft Active Directory for the last 24 hours.

Windows System Audit Policy Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	Shows all Microsoft system audit policy changes.
Events by Certain Object - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This report displays events by device group (default /Host/Application).
Events by Device Group - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This report displays events by device group (default /Firewall).
Events by Outcome - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 2 Audit Events/	This report displays events by category outcome (default /Success).
Resource Exhaustion Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes).
Resource Exhaustion Detected on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain) .
Security Log is Full	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	This report shows windows events indicating that the security log is full.
Syslog Restart Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Shows all restarts of syslog on systems.
Unable to Log Events to Security Log	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	This report retrieves windows events indicating inability to log events to security log.

Device Logging Review	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 6 Audit Review, Analysis, and Reporting/	This report shows the different products that are logging to ArcSight ESM.
Clock Synchronization Issues	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This report displays all events in which there are clock synchronization issues between the deviceReceiptTime and agentTime, or the event endTime and managerReceiptTime. The report is ordered first by the agent information and then by the device information.
Clock Synchronization Issues - Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 8 Time Stamps/	This report displays a summary of the number of events for each device that had clock synchronization issues. The report is ordered first by the number of problematic agent-device time events and then by the number of problematic end-manager time events.
Audit Log Cleared	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows all events where an audit log was cleared from a host. Before running this report make sure the Rule : "Audit Log Cleared" is enabled and deployed.
Audit Log Cleared per Attacker User Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows all events where an audit log was cleared by an attacker user name. Before running this report make sure the Rule : "Audit Log Cleared" is enabled and deployed.
Audit Log Cleared per Attacker and Target	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows all events where audit logs were cleared from a host by an attacker. Before running this report make sure the Rule : "Audit Log Cleared" is enabled and deployed.
Audit Log Cleared per Target User Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Shows all events where an audit log was cleared by a target user name. Before running this report make sure the Rule : "Audit Log Cleared" is enabled and deployed.
FISMA Reports Accessed	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This report shows all the accessed FISMA reports ,who accessed those reports and when.

FISMA Reports Accessed by Report - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This report shows all the accessed FISMA reports events by specific report(default/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins).
FISMA Reports Accessed by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This query retrieves all the FISMA reports accessedby specific user (default admin).
Information System Audit Tool Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This report shows logins, both successes and failed, to information system audit tools (ArcSight).
Information System Audit Tool Logins by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	This report shows logins, both successes and failed, to information system audit tools (ArcSight) by specific user (default admin).
All Actions by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows all action events by user. The user has to be specified at report runtime (default admin).
All Administrator Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows all administrative action events by ip address. Administrative users are defined by the filter Administrative User. IP Address has to be specified at run time default 127.0.0.1.
All User Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows all non administrative action events by ip address. Administrative users are defined by the filter Administrative User. The ip address has to be specified at report runtime (default 127.0.0.1)
Failed Actions by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows failedaction events by user. The user has to be specified at report runtime (default admin).
Failed Administrative Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows failed administrative action events by IP address. Administrative users are defined by the filter Administrative User. The IP address has to be specified at report runtime (default 127.0.0.1).

Failed User Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows failed administrative action events by IP address. Administrative users are defined by the filter Administrative User. The IP address has to be specified at report runtime (default 127.0.0.1).
Logins and Logouts by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report provides a listing of logins and logouts per target or attacker user name (default admin).
Successful Actions by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows successfulaction events by user. The user has to be specified at report runtime (default admin).
Successful Administrative Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows successful administrative action events by IP address. Administrative users are defined by the filter Administrative User. The IP address has to be specified at report runtime (default 127.0.0.1).
Successful User Actions by IP Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows successful non administrative action events by IP address. Administrative users are defined by the filter Administrative User. The IP address has to be specified at report runtime (default 127.0.0.1).
Trend of Failed Administrative Actions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows different aspects of the trend of failed administrative actions. Administrative accounts are defined by the filter Administrative User.
Trend of Failed Administrative Actions per Product	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This report shows different aspects of the trend of failed administrative actions. The report can be run up to 31 days back. Administrative accounts are defined by the filter Administrative User.
All Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity flagged as information leakage.
Encrypted Communication Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a source is accessing sensitive information, although encrypted.

Former Employee Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity which involved former employees and flagged as information leakage.
Inactive Employee Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity which involved inactive employees and flagged as information leakage.
Information Disclosure Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	Shows information disclosure vulnerabilities identified on the last 24 hours.
Monitored Accounts Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity which involved monitored accounts and flagged as information leakage.
New Hire Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity which new hire employees and flagged as information leakage.
Organizational Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak.
Organizational Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate an organizational information leak on network domain ,The network domain has to be specified at report runtime (default Development). Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Organizational Records Information Leaks Originated from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows the communications which were classified as information leaks of organizational records originated from third party.

Personal Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak.
Personal Information Leaks Originated from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak originated from third party.
Personal Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows events which indicate a personal information leak on network domain ,The network domain has to be specified at report runtime (default Development). Assets have to be modeled in ESM and categorized with one or more Asset Categories under the /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains group.
Privileged Accounts Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This report shows all activity that involved privileged accounts and flagged as information leakage.
Configuration Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to specific network domain (default operations).
Daily Report - Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the number of times changes were made to operating systems.
Daily Report - Configuration Modifications by Host Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to specific host name (default localhost).
Daily Report - Configuration Modifications by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays all configuration modificationsby specific user (default admin).

Daily Trend - Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows several top-level views related to configuration modifications.
Database Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows database configuration changes.
Firewall Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows several top-level views related to firewall configuration modifications.
Firewall Configuration Modifications by Firewall - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications by firewall host name (default localhost).
Firewall Configuration Modifications by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any firewall by specific user (default admin).
List of Firewall Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any firewall.
List of Network Device Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any network equipment. Default time window: Last 24 hours.
List of Network IDS Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows any configuration modifications of any network IDS. Default time window: Last 24 hours.
Network Device Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows several top-level views of configuration modifications of any network equipment.

Network IDS Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows several top-level views related to network IDS configuration modifications.
Operating Systems Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the number of times changes were made to operating systems.
Operating Systems Configuration Modifications by Host Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the number of times changes were made to operating systems by specific host (default localhost).
Operating Systems Configuration Modifications by Process Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times changes were made to operating system specific process (default winlogon).
Operating Systems Configuration Modifications by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the number of times changes were made to operating systems by specific user (default admin).
Unsuccessful Operating Systems Configuration Modifications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows the number of times unsuccessful changes attempted on operating systems.
Weekly Report - Configuration Modifications by Host Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to specific host name (default localhost) on the last 7 days.
Weekly Report - Configuration Modifications by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Displays the changes were made to specific user name (default admin) on the last 7 days.

Weekly Trend - Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Shows several top-level views weekly configuration modifications.
Account Change Details by Attacker User Name -Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts by specific attacker user name (default admin).
Account Change Details by Host Name -Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events when an account was attempted to be changed on specific host name (default localhost).
Account Change Details by Target User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events regarding changes to accounts by specific target user name (default admin).
Account Change Details in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Lists details of events when an account was attempted to be changed on specific network domain (default operations).
Code Signing Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Displays all the code signingflaws Detected.
Successful Removal of Access Rights - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This report shows the removal of access rights from a host resource in a particular domain.
Successful Removal of Access Rights by Target User Name Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	This report shows all the removal of access rights by target user name (default admin).
New System Count by FIPS-199 Security Objective	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the number of new systems with FIPS-199 categorizations in the last month.

New System Count by FIPS-199 or NIST 800-53 Criticality	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the number of new systems with FIPS-199 or NIST 800-53 categorizations in the last month.
New System Count by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the number of new systems categorized under FIPS-199 or NIST800-53 grouped by their network domains in the last month.
New Systems by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	This report shows an overview of the new assets by their network domains on specific time (default Production network domain and last month).
Asset Creation	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of newly created assets.
Asset Deletion	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of deleted assets.
Asset Identification Report	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows all assets and their respective network domain.
Asset Modification	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of modified assets.
Assets by Application Type	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets by application type. This report may (and should) be focused based on the application type of interest. Results are sorted by creation time.
Assets by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the network domain of interest. Results are sorted by creation time.

Assets by Network Zone	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This report provides an overview of assets on ESM grouped by zone.
Assets by Owners	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of assets by owners.
Assets without Assigned Owner	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides a listing of assets without assigned owner.
Classification of Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows the asset classifications.
Critical Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.
Criticality of Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Shows the asset criticality.
E-Authentication Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides an overview of E-Authentication Levels on the organization.
Non-Operating System Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets which categorized as non OS Systems. This report may (and should) be focused based on the application type of interest. Results are sorted by creation time.
Operating System Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	Provides the listing of all the assets which categorized as OS Systems. This report may (and should) be focused based on the application type of interest. Results are sorted by creation time.

Software Products on Specific Asset - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This report shows all software products detected on a specific asset in the last two weeks. The asset can be identified using either its address or its hostname.
Software Summary by Network Domain in Last 2 Weeks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This report lists the software detected in your environment during the last two weeks, sorted by by business network domain.
Software Summary by Zone in Last 2 Weeks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This report lists the software detected in your environment by zone during the last two weeks.
Software Summary in Last 2 Weeks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This report lists the software detected in your environment.
Critical Asset Details on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report lists all the critical assets which have been categorized with a criticality of high or very-high on specific network domain (default development). It can be used to identify key assets to implement the business continuity process.
Fault Logs on Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows events indicating a process has failed to execute in the expected way on critical machines.
Information System Failures per Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows the critical information system which generated error log entries.
Shutdown Machine not Started more than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown machines which not started more than policy standard.
Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on the last day.

Shutdown of Critical Machines on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows all shutdown events of machines categorized as critical on specific network domain on the last day.
Weekly Trend - Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This report shows a weekly trend of critical machines shutdown.
Identity Management Policy Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 1 Identification and Authentication Policy and Procedures/	Lists all the changes to identity management policies.
Identity Management Policy Violations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 1 Identification and Authentication Policy and Procedures/	Lists all the violations to identity management policy.
Attempted Default Vendor Accounts - Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows summary views of events and systems when a vendor supplied user account is attempted by a user to login.
Default Vendor Account Involved on Information Leaks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report shows all activity which involved default vendor accounts and flagged as information leakage.
Default Vendor Account Involved on Internal Reconnaissance	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report shows all activity which involved default vendor accounts and flagged as internal reconnaissance.
Detail Specific Default Vendor Account Uses	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows all logins using a specific vendor supplied user account.

Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows different aspects of the trend of unsuccessful administrative logins in the last 16 weeks.
Non Multi Factor Access by Admin Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report shows events indicating a non multi factor authentication by admin accounts. Before running this report please make sure the following rule is deployed and enabled : Non Multi Factor Access by Admin Account Also please ensure that your multi factor authentication devices are added to the following active list : /All Active Lists/ArcSight Solutions/FISMA/Multi Factor Authentication Devices
Number of Successful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the hourly number of successful administrative logins and a list of those logins, grouped by user and host information.
Number of Successful Administrative Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of successful administrative user logins per hour.
Number of Successful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of successful non-administrative user logins every day over the past week.
Number of Successful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of successfulnon-administrative user logins per hour.
Number of Unsuccessful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the hourly number of unsuccessful administrative logins, and a listing of those attempts, grouped by user and host information.

Number of Unsuccessful Administrative Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of unsuccessful administrative user logins every hour over the past day.
Number of Unsuccessful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of unsuccessful non-administrative user logins every day over the past week.
Number of Unsuccessful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows the number of unsuccessfulnon-administrative user logins every hour over the past day.
Observed Direct Root or Administrator	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows systems when direct root or administrator account is observed.
Replay Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows events identifying replay attacks based on Microsoft event ID 4649.
Same User Using Different User Names	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report shows users that have logged in using different user names.
Successful Administrative Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful administrative login attempts.

Successful Administrative Logins by Attacker Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful administrative login attempts by specific attacker host (default localhost).
Successful Administrative Logins by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful administrative login attempts by target host (default localhost).
Successful Default Vendor Account Used - Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows high level summary views of events when a vendor-supplied user account is used to login.
Successful Local Administrative Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful local administrative login attempts.
Successful User Local Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful non-administrative user local login attempts.
Successful User Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful non-administrative user login attempts.
Successful User Logins by Attacker Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successfulnon-administrative user login attempts by specific attacker host (default localhost).

Successful User Logins by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful non-administrative user login attempts by target host (default localhost).
Successful User Logins by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report provides a listing of successful user login attempts by User(default admin).
Systems Accessed by Default Vendor Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Shows all systems that users have tried to access as a default vendor account.
User Logged in from different IP Addresses	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This report shows single user names that have been used to login from different IP addresses.
Accepted Accesses Through AAA Server	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report displays all the accepted accesses through AAA Server.
All DHCP Leases by Particular Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all information about DHCP leases by a particular host name in the last 24 hours.
All DHCP Leases by Particular Offered IPv4 Address	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all information about DHCP leases by a particular offered IP address in the last 24 hours.

All DHCP Leases by Particular Offered IPv6 Address	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all information about DHCP leases by a particular offered IPv6 address in the last 24 hours.
All DHCP Leases by Particular Source MAC Address	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all information about DHCP leases by a particular source MAC address in the last 24 hours.
All Daily DHCP Critical Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all information about DHCP critical events in the last 24 hours.
DHCP Lease Statistics in Last 7 Days	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents all DHCP leases in the last 7 days.
MAC Count per Leased IP	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report presents the MAC count per leased IP.
Rejected Accesses Through AAA Server	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This report displays all the rejected accesses through AAA Server.
All Password Change Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Provides a list of all password change events, ordered by the time in which they occurred.
All Password Change Events by User - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Provides a list of all password change events, ordered by the time in which they occurred by specific user (default admin).

Failed Password Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Displays failed password change events.
Minimum Password Age Changed to Less than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This report shows events when minimum password age changed to Less than policy standard (default 60 days), you can change the default by editing referenced rule condition : "passwordAgedtoInt < 60" from 60 to different value which reflects your policy standard.
Minimum Password Length Changed to Less than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This report shows events when minimum password age changed to Less than policy standard (default 15 days), you can change the default by editing referenced rule condition : "New Minimum Password Length< 15" from 15 to different value which reflects your policy standard.
Password Policy Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	This report shows all password policy changes based on windows events.
Password Spray Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Shows password spray attack on windows systems. Before running this report please make sure the following rule : Password Spray Attack is enabled and deployed.
Passwords not Changed for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Lists passwords that were not changed for longer than the policy standard.
Successful Password Changes	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Displays successful password change events.
Unsecured Password Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Displays unsecured password events.

Average Time to Resolution - By Case Severity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report will show the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.
Average Time to Resolution - By Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report shows the average time to resolution of all the closed cases by day.This report should be run once a week and reported to management.
Average Time to Resolution - By User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report shows how long it is taking individuals to close their cases. This report should be run once a week and reported to management.
Cases by Stage	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report provides an overview of all cases and their current stages.
Open Cases by Control Family	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report shows all currently open cases by Control Family.
Open Cases by Control Family and Severity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report shows all currently open cases by control Family and severity.
Open Cases by Owner	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report provides a breakdown by owner of all open cases.
Open Cases by Severity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This report shows all currently open cases by severity.
Attacks and Suspicious Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events targeting a particular Network Domain (default development). The Network Domain of interest should be specified at report runtime.
Attacks and Suspicious Activities by Attacker Address - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by attacker address, (default 127.0.0.1).

Attacks and Suspicious Activities by Attacker Zone - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by attacker zone (default RFC1918: 10.0.0.0-10.255.255.255).
Attacks and Suspicious Activities by Country	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by country.
Attacks and Suspicious Activities by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by target host, (default localhost).
Attacks and Suspicious Activities by Target Port - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by target port (default 80).
Attacks and Suspicious Activities by Target Zone - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events by target zone (default RFC1918: 10.0.0.0-10.255.255.255).
Attacks and Suspicious Activities from a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events from a particular Network Domain (default development). The Network Domain of interest should be specified at report runtime.
Attacks and Suspicious Activities from specific Country - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a listing of all hostile or suspicious events from specific country (country code should be provided on lower case,default us).
Count of Attacks and Suspicious Activities per Attacker Machine	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This reports shows a count of attack and suspicious activity events per attacker machine.
Count of Attacks and Suspicious Activities per Target Machine	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This reports shows a count of attack and suspicious activity events per target machine.

Daily Report - Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all attack and suspicious activity events.
High Priority Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows events in which the Priority field is 10.
Internal Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all internal attack and suspicious activity events.
Internal Recon Activities Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows an overview of internal recon activity.
Reconnaissance Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows all reconnaissance activity.
Reconnaissance Activities From a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all reconnaissance activities From a Network Domain events from a particular Network Domain (default development). The Network Domain of interest should be specified at report runtime.
Reconnaissance Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a list of all reconnaissance activities Targeting a Network Domain activity events targeting a particular Network Domain (default development). The Network Domain of interest should be specified at report runtime.
Reconnaissance Activities from specific Country - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a listing of all reconnaissance activities from specific country(country code should be provided on lower case,default us).
Weekly Report - Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a weekly trend of attacks and suspicious activity
Weekly Trend - Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This report shows a weekly trend of attacks and suspicious activity

Critical Machine Configuration Modifications at Unscheduled Time	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This report shows unscheduled critical machine configuration modifications in the last 24 hours.
Network Device Configuration Modifications at Unscheduled Time	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This report shows unscheduled network device configuration modifications in the last 24 hours.
System Shutdown or Restart at Unscheduled Time	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This report shows unscheduled restarts of hosts in the last 24 hours.
Unscheduled Change in Status of Service	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This report shows the starting or stopping of services outside of scheduled maintenance windows in the last 24 hours.
All Actions by User at Maintenance Time - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 3 Maintenance Tools/	This report shows all actions by specific user at maintenance time ,username has to be specified at report runtime (default admin). Note : This report displays data based on "Maintenance Window" Filter which by default defined to Sunday morning, 3:00 AM to 3:59 AM, and Wednesday morning, 4:00 AM to 4:59 AM ,in order for this report to generate data you should make sure that the start time and end time of the report includes the "Maintenance Window".
Failures at Maintenance Time by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 3 Maintenance Tools/	This report shows allfailure events in maintenance time on specific hostname,hostname has to be specified at report runtime (default localhost). Note : This report displays data based on "Maintenance Window" Filter which by default defined to Sunday morning, 3:00 AM to 3:59 AM, and Wednesday morning, 4:00 AM to 4:59 AM ,in order for this report to generate data you should make sure that the start time and end time of the report includes the "Maintenance Window".
All Specific Host Actions which Originated from Remote at Maintenance Time - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 4 Nonlocal Maintenance/	This report shows all actions originated from remote on specific host at maintenance time,hostname has to be specified at report runtime (default localhost).

Removable Media Accesses after Work Hours	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	Shows all the removable accesses after work hours.
Successful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of successfulogin attempts to network domain, The network domain has to be specified at report runtime (default Development).
Unsuccessful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	This report provides a listing of unsuccessful login attempts to network domain, The network domain has to be specified at report runtime (default Development).
Removable Media Plugged In Multiple Assets in Short Period of Time	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	This report shows removable media plugged In multiple assets in short period of time. Before running this report please make sure the following rule: Removable Media Plugged In Multiple Assets in Short Period of Time is enabled and deployed.
After Hours Successful Monitored Accounts Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all after hours successful new hire logins within the last day.
After Hours Successful New Hire Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all after hours successful new hire logins within the last day.
All Successful Actions by Monitored Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Shows details of all all successful actions taken by monitored accounts.
Monitored Accounts Email Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all email activity by monitored accounts.
Monitored Accounts Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all the identified internet activity performed by monitored accounts.
New Hire Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all the identified internet activity performed by new users.

New Hires Email Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all email activity by new hires.
Summary of Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This report shows a summary of attacks and suspicious events by new hires.
Suspicious Activity by Monitored Accounts	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all the identified suspicious activity performed by monitored accounts.
Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all the identified suspicious activity performed by new users.
Unsuccessful Monitored Accounts Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Shows details of all failed monitored accounts logins within the last day.
Unsuccessful New Hire Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	Displays all after hours unsuccessful new hire logins within the last day.
List of Terminated Employees on the Last Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 4 Personnel Termination/	Displays all terminated employees on the last day. Before running this report make sure this rule ""Former Employee Account Detected" is enabled and deployed .
Building Access and Leave by Contractors	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 7 External Personnel Security/	Shows successful building access and leave events by contractors.
Building Access and Leave by Visitors	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 7 External Personnel Security/	Shows successful building access and leave events by visitors
Building Access and Leave by Building	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by building,the buildinghas to be specified at report runtime.

Building Access and Leave by User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access and leave events by user (default admin).
Failed After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the failed physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows failed attempts to enter a building at any time.
Successful After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows the successful physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Successful Building Access Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access events.
Successful Building Access Granting	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building access-granting events.
Successful Building Leaving Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Shows successful building leave events.
Machines Conducting Policy Breaches	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows machines which were involved in policy breaches.
Machines Conducting Policy Violations	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows machines which were involved in policy violations.

Policy Violations Originated from Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Provides a listing of events categorized by ArcSight as policy violations which originated from various Network Domains by Asset. This report may (and should) be focused based on the Network Domain of interest.
Policy Violations on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This report may (and should) be focused based on the Network Domain of interest.
Top 20 Policy Breaches Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 20 policy breaches events.
Top 20 Policy Violation Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	Shows the top 20 policy violation events.
Email Activity Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays overview of email activity on the organization.
Email Activity by User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all email activity by specific user (The user email has to be specified at report runtime).
Former Employee Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified internet activity performed by former employees. Before running this report please make sure the following Rule : Former Employee Account Detectedis enabled and deployed.
New Hire Account Added to Groups	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all new hires account added to groups.
Non Privileged Accounts Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified internet activity performed by non privileged accounts.
Privileged Accounts Internet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Displays all the identified internet activity performed by privileged accounts.

Severe Information Disclosure Vulnerabilities on PII Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Shows information disclosure vulnerabilities identified on the last 24 hours on PII assets.
Targeted Recon Activity from the Same Country against Multiple PII Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report shows all activity flagged as targeted recon activity from the same country against Multiple PII Assets on short period of time. Before running this report make sure that this rule : "Targeted Recon Activity from the same Country against Multiple PII Assets" is enabled and deployed.
Unauthorized Access of Information on PII Asset	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report shows all activity flagged as unauthorized access of information on PII assets.
Unsuccessful Logins by the Same User to Multiple PII Assets on Short Period	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This report shows all activity flagged as unsuccessful logins by the same user to multiple PII assets on short period. Before running this report make sure that this rule : "Frequent Unsuccessful Logins by User Name to Multiple PII Assets on Short Period" is enabled and deployed.
Internal Malicious Code Sources	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	Shows information about the internal sources of malicious code activities.
Potential Insider Threat Campaign Against the Organization	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This report shows critical attacks launched by multiple internal attackers against the same network domain using the same pattern of attack. Before running this report please make sure this rule "Insider Threat" is enabled and deployed.
Shared Machines among Test Environment and Personal Identifiable Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	Returns all assets that are shared between Test environment and Personal Identifiable assets.
Daily Report - Overflow Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows overflow vulnerabilities identified on the last 24 hours.

Daily Report - SQL Injection Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Shows SQL injection vulnerabilities identified on the last 24 hours.
Daily Report - Vulnerabilities by CVE ID	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Displays vulnerability overview detected by vulnerability scanners for the last day ,CVE ID should be provided at report runtime.
Daily Report - Vulnerabilities by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Displays vulnerability overview by host name for the last day (default localhost).
Daily Report - Vulnerability Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Provides overview of the vulnerability summary in the last 24 hours.
Daily Report - XSRF Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Shows XSRF vulnerabilities identified on the last 24 hours.
Daily Report - XSS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Shows XSS vulnerabilities identified on the last 24 hours.
Daily Report- CVSS Score Greater than or Equal to 8 Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Provides overview of vulnerabilities with CVSS >=8 on the last 24 hours.
List of Vulnerability Scanners not run for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	This report shows vulnerability scanners which not run for longer than policy standard. Policy standardis defined by the TTL in the active list "Vulnerability Scanners" (default 60 days). Before running this report please make sure the following rules are enabled and deployed : 1.Vulnerability Scanner didn't Run for Longer than Policy Standard 2.Vulnerability Scans
Missing Security Patches Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA-5 Vulnerability Scanning/	Shows missing security patches summary. Default time window: Last 24 hours.

Top 10 Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerabilities on FISMA assets.
Top 10 Vulnerable Assets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerable IT Governance assets.
Top 10 Vulnerable Assets on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows the top 10 vulnerable IT assets on network domain (default Development Network Domain)
Vulnerabilities Summary on Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerability summary on specific network domain (default development) on the last day.
Weekly Report - Overflow Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows overflow vulnerabilities identified on the last 7 days.
Weekly Report - SQL Injection Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows SQL injection vulnerabilities identified on the last 7 days.
Weekly Report - Vulnerabilities by CVE ID	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Displays vulnerability overview by cve id for the last 7 days, cve id should be provided at report runtime.
Weekly Report - Vulnerabilities by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Displays vulnerability overview by host name for the last 7 days (default localhost).
Weekly Report - Vulnerability Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of the vulnerability summary in the las 7 days.
Weekly Report - XSRF Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows XSRF vulnerabilities identified on the last 7 days.

Weekly Report - XSS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Shows XSS vulnerabilities identified on the last 7 days.
Weekly Report- CVSS Score Greater than or Equal to 8 Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Provides overview of vulnerabilities with CVSS >=8 on the last 7 days.
Daily Report - Successful DoS Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report shows details of successful denial of service attacks.
Daily Report - Unsuccessful and Attempted DoS Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report shows details of unsuccessful and attempted denial of serviceattacks.
Daily Report- Count of DoS Attacks per Hour	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report shows a list of top attackers responsible for initiating denial of service attacks.
Daily Report- Top DoS Attackers	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report shows a list of top attackers responsible for initiating denial of service attacks.
Daily Report- Top DoS Targets	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report shows hosts which were targeted the most with a denial of service attack.
Weekly Trend - DoS Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This report displays a weekly overview of DoS attack events.
Blocked Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the blocked outbound firewall traffic originating from assets in the indicated Network Domain of interest.

Blocked Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the outbound firewall traffic originating from assets in the indicated Network Domain of interest.
Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report provides a listing of the inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Open Firewall Port Details	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report gives details of all the ports that are allowed to pass through various firewalls.
Reconnaissance from Third Party Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report shows reconnaissance activity from assets in the Business Associate domain targeting assets in the PHI domain.
Third-Party Incidents - Closed Cases	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report shows all cases involving third-party systems that have been closed. third-party cases defined under the following case URI : /All Cases/ArcSight Solutions/FISMA/Third-Party Incidents
Third-Party Incidents - Open Cases	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This report shows all cases involving third-party systems that are still open. third-party cases defined under the following case URI : /All Cases/ArcSight Solutions/FISMA/Third-Party Incidents
Inbound Insecure Transmissions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.

Internal Insecure Service Providers	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all internal providers of insecure services.
Internal Insecure Transmissions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all internal traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Outbound Insecure Transmissions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Lists all outbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Traffic Anomaly on Application Layer	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This report shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This report shows traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This report shows traffic anomaly on transport layer.
Unencrypted Services by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Returns all unencrypted services by a particular host name (by default localhost) identified in the last 24 hours using vulnerability and port scanning events.

Daily Report - Cryptographic Hash Algorithm Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic hash algorithm vulnerabilities that have been detected.
Daily Report - Cryptographic Public Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic public key vulnerabilities that have been detected.
Daily Report - Cryptographic Symmetric Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic symmetric key vulnerabilities that have been detected.
Daily Report - Cryptographic Weak Protocol Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	This report shows all cryptographic weak protocol vulnerabilities that has been detected.
Daily Report - SSH Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all SSL vulnerabilities that have been detected.
Daily Report - SSL|TLS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all SSL/TLS vulnerabilities that have been detected.
Daily Report - VPN Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all VPN vulnerabilities that have been detected.
Weekly Report - Cryptographic Hash Algorithm Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic hash algorithm vulnerabilities that have been detected on the last 7 days.
Weekly Report - Cryptographic Public Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic public key vulnerabilities that have been detected on the last 7 days.

Weekly Report - Cryptographic Symmetric Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic symmetric key vulnerabilities that have been detected on the last 7 days.
Weekly Report - Cryptographic Weak Protocol Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all cryptographic weak protocol vulnerabilities that have been detected on the last 7 days.
Weekly Report - SSH Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all SSH vulnerabilities that have been detected on the last 7 days.
Weekly Report - SSL|TLS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all SSL/TLS vulnerabilities that have been detected on the last 7 days.
Weekly Report - VPN Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Shows all VPN vulnerabilities that have been detected on the last 7 days.
Invalid or Expired Certificate	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Shows incidents which indicate that an invalid or expired certificate was detected.
Mobile Code Detection	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-18 Mobile Code/	This report displays mobile code detected based on snort and nessus signatures which found on the following active list : Mobile Code Detection Signatures.
Daily Report - VOIP Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Shows voip vulnerabilities identified on the last 24 hours.
Traffic Anomaly on VOIP Applications	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This report shows traffic anomaly related to VOIP applications.

VOIP Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This report shows a list of all VOIP attack and suspicious activity events on the last 24 hours.
Weekly Report - VOIP Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Shows voip vulnerabilities identified on the last 7 days.
DNS Queries Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This report shows a DNS queries overview on the last day,This report is based on DNS Bind events.
DNS Queries by Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This report shows a DNS queries by specific DNS domain name on the last day, domain name should provided at report run time. This report is based on DNS Bind events.
DNS Queries by Originator IP	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This report shows a DNS queries by specific originator IP on the last day, originator IP should be provided at report run time, This report is based on DNS Bind events.
Weird DNS Queries Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This report shows overview of weird DNS queries, it's based on DNS Bind events. Weird DNS query is defined by this rule: "DNS Abnormal Queries Detected" where the length of the domain by default is more than 60 characters and it contains more than 5 numbers. Before running this report please make sure the following Rule "DNS Abnormal Queries Detected" is enabled and deployed .
Information Interception Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This report shows all information interception activity.

Redirection Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This report shows all redirection attacks
Honeypot Interaction Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This report shows all honeypots events received on the last 24 hours.
Daily Report - Insecure Cryptographic Storage	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Shows all insecure cryptographic assets events identified in the last 24 hours.
Weekly Report - Insecure Cryptographic Storage	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Shows all insecure cryptographic assets events identified in the last 7 days.
Covert Channel Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-31 Covert Channel Analysis/	This report shows all covert channel activity.
Meltdown|Spectre Vulnerability Detected	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	This report displays Meltdown|Spectre related flaws reported by vulnerability scanners.
Daily Report-Anti-Virus Stopped or Paused	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all events when Anti-Virus is stopped or paused in the last day.
Failed Anti-Virus Updates	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all the failed Anti-Virus updates on the last 24 hours.
Weekly Report-Anti-Virus Stopped or Paused	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Shows all events when Anti-Virus is stopped or paused in the last week.

Failed Virus Removal Events	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of failed virus removal events on the last 24 hours.
Hacker Tools Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of hacker tools detected on the last 24 hours. Before running this report make sure the following rule : Hacker Tool Detected is enabled and deployed.
Shellcode Executions	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of shellcode execution detected on the last 24 hours.
Spyware Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows an overview of spyware activities.
Trojan Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of trojan activities detected on the last 24 hours.
Virus Activities Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of virus activities detected on systems sorted by virus.
Virus Activity by Target Host - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of virus activities detected on a specific host on the last day, host name should be specific at report runtime (default localhost).
Virus Activity by Virus Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of virus activities by specific virus name on the last day, virus name should be specific at report runtime.
Worm Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Shows a summary of worm activities detected on the last 24 hours.

Email Attacks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This report shows all email attacks
Email Traffic with Competitors	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	Displays all email traffic with competitors.
Installed Windows Services by Host Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This report lists all the installed windows systems events by specific host (default localhost) on the last 24 hours.
Phishing Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This report shows all email phishing activity in the last day.
Possible Botnet Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This report shows possible C&C Activity on the last 24 hours. Before running this report please make sure the following rule : Possible Botnet Activity is enabled and deployed.
User Logged in from Two Countries	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This report shows user names that have been used to login from two different countries. This may indicate user name sharing. Before running this report please make sure the following rule : User Logged in from Two Countries is enabled and deployed .
Daily Report - BIOS Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Shows BIOS flaws identified on the last 24 hours.
File Creationsby Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all created file detected based on reports from the File Integrity Checker on specific host (default localhost) Default time window: Last 24 hours.

File Deletionsby Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all deleted file detected based on reports from the File Integrity Checker on specific host (default localhost) Default time window: Last 24 hours.
File Integrity Changes by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all file changes detected based on reports from the File Integrity Checker on specific host (default localhost) Default time window: Last 24 hours.
File Integrity Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all file changes detected based on reports from the File Integrity Checker on specific domain (default development) Default time window: Last 24 hours.
Integrity Tools	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows integrity tools reporting to ArcSight ESM based on ArcSight Categorizations. Default time window: Last 24 hours.
Software Changes by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all changes to any software installed by host name (default localhost).
Software Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	This report shows all changes to any software installed on specific network domain (default development).
Weekly Report - BIOS Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Shows BIOS flaws identified on the last 7 days.

Spam Activity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This report shows all email spam activity in the last day.
Command Injection on HTTP Request	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	Shows a summary of command injection on HTTP Requests detected on the last 24 hours. Before running this report make sure the following rule : Command Injection on HTTP Request is enabled and deployed.
Daily Report - ASLR or Data Execution Prevention Bypass Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Shows an ASLR or Data Execution Prevention Bypass Flaws on the last 24 hours.
Disabled Data Execution Prevention (DEP) Mechanism	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	This report shows events on the last 24 hours indicating that a data execution prevention is disabled ,by default is based on Nessus signature id 24282.
Weekly Report - ASLR or Data Execution Prevention Bypass Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Shows an ASLR or Data Execution Prevention Bypass Flaws on the last 7 days.
Attempted File Changes in Development Originated from Other Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Displays attempts to change a file on a host in the development segment from a source that is not in the development segment.
File Changes in Development	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report displays a count of the number of creations, deletions and modifications of files on systems in the development network domain.
Successful Administrative Logins to Development Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report displays all successful logins to assets categorized as Development, that were done with an administrator account.

Successful User Logins to Development Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report displays all successful non-administrative logins to assets categorized as Development.
Unsuccessful Administrative Logins to Development Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report displays all failed logins with an administrative account to assets categorized asDevelopment.
Unsuccessful User Logins to Development Systems	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	This report displays all failed logins with a non-administrative account to assets categorized as Development.
New Development Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	This report displays all the new development vulnerabilities that identified on last scan. Before running this report make sure the following rule "Vulnerabilities on Development" is enabled and deployed.
Non Fixed Development Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	This report displays all the persistent development vulnerabilities that identified on reoccurring scans and not fixed by developers. Before running this report make sure : 1. the following rule "Vulnerabilities on Development" is enabled and deployed. 2.the TTL on this active list :Vulnerabilities on Development Environment is equal to the vulnerability scan frequency on the organization.
Disabled User Account Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Fires when a disabled user account is detected.
Enabled User Account Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Fires when a user account is enabled.

Former Employee Account Activity	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Looks for any activity of users that have been placed on the Former Employees active list. This rule creates a case for each unique user name that is attempted in the ArcSight Solutions/Compliance Insight Package folder in the case tree.
Former Employee Account Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Detects events that list former employee accounts. When triggered, the rule adds as well as deletes users from the appropriate active lists.
Former Employee User Account Access Attempt	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Detects any authentication event, whether failed or successful, where the username has been placed on the Former Employees active list. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.
Inactive User Account Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Fires every time an entry ages out of the Active Accounts active list,the user name will be added to the Stale Accounts active list.
Login Activity by a Stale Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies login activities by accounts that are on the Stale Accounts active list.
Monitored Account Added to group	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Triggers when a monitored account is added to group. Monitored accounts is defined using this active list : "Monitored Accounts"
Monitored Account Modification	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Triggers when a monitored account is modfied. Monitored accounts is defined using this active list : "Monitored Accounts"
Monitored Account Removed from group	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Triggers when a monitored account is removed from group. Monitored accounts is defined using this active list : "Monitored Accounts"
Privileged Account Changes	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Fires whenever an access/authorization change is attempted to be made to an administrative account. A case is created for each such incident.
Removal of Access Rights	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Triggers when events indicating a removal of access rights happens.

Suspicious Activities by Former Employee	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Detects Suspicious Activities events, where the username has been placed on the Former Employees active list. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.
Suspicious Activities by a Stale Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Identifies suspicious activities by accounts that are on the Stale Accounts active list.
User Logged in - Added to Active Accounts List	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	Adds a user account to the Active Users session list upon a successful login.
Unauthorized Access to High Impact Systems	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 3 Access Enforcement/	This rule detects an unauthorized access to the high impact systems.
Communication between Non Classified Machines and Classified Machines Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	This rule fires any time communication between non classified machines and classified machines is detected.
High to Low Classified Traffic Information Leak	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	Looks for information leak events which originated from a high-security classified system.
Communication between Production and Development Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This rule fires any time communication between a production asset and a machine in the development domain is detected.
Communication between Sensitive Asset and Test Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This rule fires any time communication between a sensitive asset and a machine in the Test domain is detected.
Communication between Sensitive Asset and Third Party Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	This rule fires any time communication between a sensitive asset and a machine in the Third Party domain is detected.

Test and Development Accounts in Production Environment	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	Detects the use of a test or development user in the production environment.
Special privileges assigned to new logon	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 6 Least Privilege/	This rule detects events which identifies when a special privileges assigned to new logon.
Account Lockout	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This rule detects account lockouts. This activity is suspicious.
Brute Force Login Attempts	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Identifies brute force login attempts.
Consecutive Unsuccessful Logins to Administrative Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This rule fires when it notices a set of 10 consecutive unsuccessful logins by an attacker and target user name pair within 5 minutes .
Frequent Unsuccessful Logins by User Name	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Fires when it notices the same user is responsible for a continuous set of unsuccessful logins.
Frequent Unsuccessful Logins from Attacker Host	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Fires when it notices a continuous set of unsuccessful logins from the same attacker host.
Frequent Unsuccessful Logins to Target Host	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Fires when it notices a high frequency of unsuccessful logins on the same target host.
Successful Attack - Brute Force Login	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	Detects successful brute force login attacks.
Unsuccessful Logins to Multiple Administrative Accounts	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 Unsuccessful Login Attempts/	This rule fires when it notices a set of 20 continuous unsuccessful logins bydifferent administrative attacker and target user pairs within 5 minutes .

RDP Session Initiated	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	Fires when an RDP session is initiated.
RDP Session Terminated	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	Fires when an RDP Session is terminated.
RDP Session is not Terminated for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-12 Session Termination/	Fires when an entry expires out of the referenced active list, signifying that the session was not terminated within the prescribed time. Time limit is defined by the TTL in the active list.
Bypassing Authentication or Authorization Flaw Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-14 Permitted Actions without Identification OR Authentication/	Fires when an authentication or authorization flaw is detected.
Disallowed Ports Access	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Triggers when traffic to a forbidden target port occurs.
Frequent Unsuccessful Administrative Logins from Remote System	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Fires when it notices the same admin user is responsible for a continuous set of unsuccessful logins from remote systems.
Successful Non VPN Remote Access	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-17 Remote Access/	Will fire and open a case for each successful non VPN remote access event.
Bluetooth Protocol Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This rule detects Bluetooth flaws reported by vulnerability scanners.
Rogue Station Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This rule detects when a rogue wireless station is detected in the network.
Wireless Malicious Traffic Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This rule detects when wireless malicious traffic is detected.

Wireless Security Protocol Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	This rule detects flaws reported by vulnerability scanners which related to wireless security protocols such as WEP,WPA,WPA2 etc..
Removable Media Detected on Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	Looks for events indicating that a removable device is detected on highly critical machine.
Possible Bitcoin Mining Activity	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-23 Data Mining Protection/	Fires when an possible bitcoin mining activity detected.
Assets that Failed Technical Compliance Check	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 2 Assessments/	Looks for events indicating that an asset failed technical compliance check.
Severely Attacked System Originated from Third Party Assets	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	This rule looks for an accumulation in severe attacks from third party assets targeting a single machine.
Information System Failures	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	This rule looks for information system failures.
Penetration Testing not Performed for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 8 Penetration Testing/	Fires when an entry expires out of the referenced active list, signifying that penetration testing didn't perform within the prescribed time. Time limit is defined by the TTL in the active list (default 60 days). Before deploying this rule make sure "Vulnerability Scans rule is enabled and deployed
Vulnerability Scans	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 8 Penetration Testing/	This rule detects vulnerability scans.
Windows Domain Policy Changed	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 1 Audit and Accountability Policy and Procedures/	This rule detects events which identifies when a windows domain policy occurred.

Resource Exhaustion Detected on Critical Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	Triggers when resource exhaustion is detected on critical machine.
FISMA Report Accessed	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Triggers when a fisma monitored FISMA report accessed. Before deploying this rule make sure to populate Monitored FISMA Reports active list with the reports that you want to monitor
FISMA Report not Accessed more than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Fires when an entry expires out of the referenced active list, signifying that the FISMA report didn't accessed within the prescribed time. Time limit is defined by the TTL in the active list (default 30 days). Before deploying this rule make sure "FISMA Report Accessed" rule is enabled and deployed .
Security Log is Full	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Triggers when security Log is full.
Unable to Log Events to Security Log	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 5 Response to Audit Process Failure/	Triggers when a security log didn't log events.
Audit Log Cleared	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 9 Protection of Audit Information/	Monitors for events on clearing of the audit log on Windows systems.
Encrypted Communication Information Leaks	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This rule looks for any encrypted communication Information Leaks on the network.
Information Disclosure Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	Triggers when information disclosure vulnerability is detected.

Organizational Data Information Leak	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This rule looks for any organizational information being sent out of the corporate network.
Personal Information Leak	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	This rule looks for any personal information being sent out of the corporate network.
Critical Change on Production Environment	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Triggers when a production environment configuration change is detected and has Very-High agent severity.
Critical Network Device Configuration Change Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Triggers when a network device configuration change is detected and has Very-High agent severity. Devices include: Firewalls VPNs Network Equipment Network Routings Network Intrusion Detection Systems
Critical Operating System Change Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Triggers when operating system change is detected on critical asset and has Very-High agent severity.
Code Signing Flaw Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	Fires when a code signing flaw is detected.
New Host Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This rule triggers when new hosts are found on the network.
New Service Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This rule fires when new services are found on machines.

Shutdown Machine not Started more than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	Fires when an entry expires out of the referenced active list, signifying that the shutdown machine didn't started within the prescribed time. Time limit is defined by the TTL in the active list (default 1 hour). Before deploying this rule make sure the following rules : 1.Shutdown of Highly Critical Machine 2.Startup of Highly Critical Machineare enabled and deployed .
Shutdown of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This rule looks for shutdown events from highly critical machines.
Shutdown of Multiple Machines on Production Environment on Short Period of Time	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This rule looks for shutdown of multiple machines on production environment on short period of time.
Startup of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This rule looks for startup events from highly critical machines.
Non Multi Factor Access by Admin Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This Rule detects events indicating a non multi factor authentication by admin accounts.
Replay Attack was Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Looks for replay attacks using windows event 4649.
Same User Using Different User Names to Login	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	This rule looks for people that are logging in with different user names.

Successful Default Vendor Account Used	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Looks for successful access to system using default user accounts.
User Logged in from different IP Addresses	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Fires when someone is using the same user name to login from different ip addresses. This may indicate user name sharing.
DHCP Critical Logging Error Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This rule detects when a DHCP critical logging error is detected.
DHCP Lease Assigned or Renewed	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This rule detects when a DHCP lease is assigned or renewed.
DHCP Lease Expired or Released	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 3 Device Identification and Authentication/	This rule detects when a DHCP lease expires or is released.
Minimum Password Age Changed to Less than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Fires when minimum password age changed to Less than policy standard (default 60 days), you can change the default by editing rule condition : "passwordAgedtoInt < 60" from 60 to different value which reflects your policy standard.
Minimum Password Length Changed to Less than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Fires when minimum password length changed to Less than policy standard (default 15 days), you can change the default by editing rule condition : "minimumPasswordLength< 15" from 15 to different value which reflects your policy standard.
Password Spray Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Detects password spray attack on windows systems.

Password not Changed for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Fires when an entry expires out of the referenced active list, signifying that the new (default) password was not changed within the prescribed time. Time limit is defined by the TTL in the active list.
Successful Password Change	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Detects when a user's password is changed.will then take the user name off the list where it was kept to track whether or not the default password was changed.
Unsecured Password Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 5 Authenticator Management/	Detects unsecured passwords.
Multiple Cases Created on Short Period	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This rule triggers when multiple cases created on short period of time.
Attacks Against Organization Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This rule looks for an exponential increase of attacks against the organization. Before deploying this rule make sure this data monitor "Attacks and Suspicious Activity per 10 Minutes" is enabled .
Recon Activity from the Same Country Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This rule looks for reconnaissance activity originated from the same country against multiple hosts on the organization.
Severely Attacked System	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This rule looks for an accumulation in severe attacks targeting a single machine.
System Shutdown or Restart at Unscheduled Time	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This rule monitors hosts that were restarted or stopped at unscheduled time.
Unscheduled Change in Status of Service	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	This rule fires any time a service on a host is changed when it is outside of a scheduled maintenance window. The maintenance window is defined by the referenced filter. A case is opened for each host on which this anomaly is detected.

Removable Media Activity by Non Identifiable Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	Looks for events indicating that a removable device is detected by non identifiable owner.
Removable Media Plugged In Multiple Assets in Short Period of Time	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 7 Media Use/	Looks for events indicating that a removable device is plugged in multiple assets in short period of time.
Consecutive Unsuccessful Logins to Monitored Account	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Personnel Security (PS)/PS- 3 Personnel Screening/	This rule fires when it notices a set of 10 consecutive unsuccessful logins by an attacker and target user name pair within 5 minutes .
After Hours Building Access by Contractors	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects building access events after business hours by contractors.
Badged Out Employee	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects when someone leaves a building and adds the user to the Badged Out active list.
Failed Access by the Same User to Multiple Buildings	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects failed physical access by the same user to multiple buildings on short period of time.
Failed Building Access	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects failed physical building access.
Local Logon from Badged Out Employee	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects a local logon event though the employee is badged out.
Potential Badge Cloned	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies when an employee is used on different buildings at the same period of time.

Potential Piggybacking Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies when an employee badge used more than one time on short period of time to access specific building.
Successful Badge In	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Identifies when an employee badges in and puts the badge id and other information on the Badged In active list.
Successful Badge Out	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Physical and Environmental Protection (PE)/PE- 6 Monitoring Physical Access/	Detects when someone leaves a building and removes the user from the badged in active list.
Multiple Policy Violations Against Assets Categorized with the Same Network Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	This rule looks for multiple policy violations against assets categorized with the same network domains. Note : In order for this rule to be triggered the assets which match the condition should be categorized with the same network domains exactly ,i.e. if asset x which has the following categories HR,PII satisfy the condition the other assets which satisfy the condition should also have exactly the same categories that asset x have(i.e. HR and PII) .
Policy Violations	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	This rule looks for policy violations.
New Hire Account Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	Detects events that list new hire accounts. When triggered, the rule adds users to the appropriate active list.
Suspicious Activities by New Hires	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 4 Rules of Behavior/	This rule identifies suspicious activity by new hires.
Frequent Unsuccessful Logins by User Name to Multiple PII Assets on Short Period	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Fires when it notices the same user is responsible for a continuous set of unsuccessful logins to multiple PII assets on short period of time.

Severe Information Disclosure Vulnerability on PII Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	Triggers when information disclosure vulnerability is detected on PHI Asset.
Targeted Recon Activity from the same Country against Multiple PII Assets	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	This rule looks for targeted reconnaissance activity from the same country against multiple PII assets on short period of time .
Insider Threat Against Single Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This rule looks for severe internal attacks and suspicious Activities against single asset.
Insider Threat Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This rule looks for an exponential increase of severe attacks originated from internal assets against the organization. Before deploying this rule make sure this data monitor "Insider Threat per 10 Minutes" is enabled .
Internal Recon Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This rule looks for internal reconnaissance activity.
Potential Insider Threat Campaign Against the organization	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	This rule looks for critical attacks launched by multiple internal attackers against the same network domain using the same pattern of attack.
Critical Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when a critical vulnerability is detected, critical vulnerability defined as vulnerability which has CVSS Score >=8.
Overflow Vulnerabilities	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when an overflow vulnerability is detected.
SQL Injection Vulnerabilities	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when SQL Injection vulnerability is detected.

Security Patch Missing	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when a security patch missing vulnerability is detected.
Specific Vulnerability Detected-Template	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when a specific CVE Id vulnerability or vendor signature ID is detected . Before enabling and deploying this rule make sure that either : 1.CVE ID is defined using deviceCustomString2 = <CVE ID> on the Conditions tab. OR 2.Signature ID is defined using device Event Class Id =<Signature ID>on the conditions tab.
Vulnerabilities on Critical Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when a vulnerability is detected on critical machine.
Vulnerability Scanner didn't Run for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Fires when an entry expires out of the referenced active list, signifying that vulnerability scanner didn't run within the prescribed time. Time limit is defined by the TTL in the active list (default 60 days). Before deploying this rule make sure "Vulnerability Scans rule is enabled and deployed
XSRF Vulnerabilities	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when XSRF vulnerability is detected.
XSS Vulnerabilities	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Triggers when XSS vulnerability is detected.
DoS Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This rule looks for DoS .
Potential Distributed DoS	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This rule looks for Potential Distributed DoS .
Excessive Blocked Firewall Traffic from the same Source	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 Boundary Protection/	This rule looks for possible excessive blocked firewall traffic from the same source.

Internal Insecure Service Provider Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	Detects when insecure protocols, such as Telnet or RSH, are used inside the network. When triggered, it adds an entry to the Internal Systems with Insecure Services active list.
Possible Traffic Anomaly	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 8 Transmission Confidentiality and Integrity/	This rule looks for possible traffic anomaly activity.
Cryptographic Hash Algorithm Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Triggers when potential cryptographic hash algorithm related vulnerability is detected.
Cryptographic Public Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Triggers when potential cryptographic public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Triggers when potential cryptographic symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Triggers when potential cryptographic weak protocol related vulnerability was detected.
SSL|TLS Vulnerabilities on Public Facing Assets	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Triggers when SSL|TLS vulnerability is detected on public-facing assets.
Invalid or Expired Certificate	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Detects invalid or expired Certificates.

One or more Rows have been Deleted from the Certificate Database	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-17 Public Key Infrastructure Certificates/	Detects if one or more rows have been deleted from the certificate database using Windows events.
Mobile Code Detection	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-18 Mobile Code/	Detects mobile code applications, by default the detection is based on Nessus and Snort signatures which found on this active list: Mobile Code Detection Signatures .
Excessive SIP 4XX Response	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Triggers when an excessive SIP 4XX responses detected.
Possible VOIP Traffic Anomaly	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	This rule looks for possible traffic anomaly activity related to VOIP assets. Before deploying this rule make sure the following rules are enabled and deployed : 1.Possible Traffic Anomaly. 2.VOIP Application Detected.
VOIP Application Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Triggers when an VOIP applicationis detected and add the following category to the detected asset /All Asset Categories/ArcSight Solution/Compliance Insight Package/Network Domain/VOIP.Its recommended to enable and deploy the following rule: VOIP Vulnerabilites Detected before enabling and deploying this rule.
VOIP Ghost Call Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Triggers when an VOIP Ghost attack is attempted.
VOIP Vulnerabilities	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	Triggers when an VOIP vulnerability is detected.
DNS Abnormal Queries Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This rule detects abnormal DNS queries, it's based on DNS BIND events, itscorrelation events used to detect possible DNS tunneling.

Possible DNS Tunneling	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-21 Secure Name Address Resolution Service (Recursive or Caching Resolver)/	This rule looks for possible DNS tunneling and it based on DNS Bind events. Before deploying this rule make sure this rule : "DNS Abnormal Queries Detected" is enabled and deployed.
Possible Information Interception	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This rule looks for attacks where information could be redirected and collected by an unintended party.
Possible Redirection Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-23 Session Authenticity/	This rule looks for attacks where information could be redirected .
Severe Honeypot Interaction Activity Increased Exponentially in less than 10 Minutes	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-26 Honeypots/	This rule looks for an exponential increase of severe honeypots events. Before deploying this rule make sure this data monitor "Severe Honeypot Interaction Activity per 10 Minutes" is enabled .
Insecure Cryptographic Storage Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Triggers when insecure cryptographic storage detected.
Possible Covert Channel	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-31 Covert Channel Analysis/	This rule looks for events indicating a covert channel is being used.
Meltdown|Spectre Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-39 Process Isolation/	Detects Meltdown and Spectre Vulnerabilities.
Failed Anti-Virus Updates	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	This rule detects failed anti-virus updates.

Security Software Stopped or Paused	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Triggers when a security software service has been disabled.
Failed Virus Removal Attempt	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This rule detects failed virus removal.
Hacker Tool Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This rule detects hacker tools based on user agent signatures.
Potential Worm Propagated Internally	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Triggers when a worm propagated internally. Before deploying this rule please make sure the following rule : Worm Detected is enabled and deployed
Shellcode Execution Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	This rule detects shellcode execution.
Spyware Detected on Critical Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Triggers when a spyware detected on critical asset.
Suspicious Internal Trojan Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Triggers when there are trojan events coming from inside the network or successful trojan events from outside the network.
Worm Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 3 Malicious Code Protection/	Triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Email Sent from High Profile User to Competitor Company	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for emails which sent from high profile users to competitor companies.

Multiple Botnet Activity to the Same C&C Center	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for multiple command and control zombies on the organization communicating with the same C&C Center. before enabling and deploying this rule please make sure the following rule : Possible Botnet Activity is enabled and deployed and the following active list : DMZ Assets includes the relevant assets.
Possible Botnet Activity	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for command and control zombies on the organization. before enabling and deploying this rule please make sure the following active list : DMZ Assets includes the relevant assets.
Possible DNS Based Zombie	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for command and control DNS zombies on the organization. before enabling and deploying this rule please make sure the following rule : Possible C&C Activity in enabled and deployed and the following active list : DMZ Assets includes the DNS relevant assets.
Possible Email Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for attacks where email activity involved .
Possible HTTP Based Zombie	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for command and control HTTP based zombies on the organization. before enabling and deploying this rule please make sure the following rule : Possible C&C Activity in enabled and deployed and the following active list : DMZ Assets includes the web relevant assets.
Possible SMTP Based Zombie	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for command and control SMTP based zombies on the organization. before enabling and deploying this rule please make sure the following rule : Possible C&C Activity in enabled and deployed and the following active list : DMZ Assets includes the SMTP relevant assets.
Possible Spear Phishing Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule identifies potential spear phishing attack, before deploying this rule please make sure to add high profile emails to the "Important Emails" active list.

Potential Email Bomb Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule identifies potential email bomb attack.
Service Installed on Critical Windows Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule looks for windows services installed on critical asset.
User Logged in from Two Countries	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 4 System Monitoring/	This rule fires when someone is using the same user name to login from two different countries. This may indicate user name sharing.
BIOS Flaws	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Triggers when a BIOS flaw is detected.
Multiple File Changes in Critical Asset on Short Period of Time	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Fires when there are multiple attempts reported by File Integrity Checker from the same source to change different files (100 by default)on critical machine on short period of time (1 minute by default).
Potential Ransomware Activity on Critical Windows Machine	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Fires when there are multiple file changes (default 100)from the same user and process on windows machine on short period of time (default 1 minute) This rule is based on windows event "4663".
Possible Spam Attack	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 8 Spam Protection/	This rule looks for email spammers.
Command Injection on HTTP Request	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	This rule detects command injections on HTTP requests.

ASLR or Data Execution Prevention Bypass Flaw on Critical Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	This rule looks if events indicating that an ASLR or data execution prevention (DEP) bypass flaw is detected.
Data Execution Prevention (DEP) is Disabled on Critical Asset	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	This rule looks if data execution prevention is disabled on critical asset ,it's based on Nessus signature id 24282.
Attempted File Changes in Development Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	Fires when it Detects multiple attempts to change a file on a host in the development segment from a source that is not in the development segment.
Vulnerabilities on Development	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-11 Developer Testing and Evaluation/	Triggers when a vulnerability is detected on development environment.
Compliance Score Update	Rule	/All Rules/ArcSight Solutions/FISMA/Overview/	This rule is triggered by other FISMA rules and updates the Compliance Score active list.
Manual Status Change	Rule	/All Rules/ArcSight Solutions/FISMA/Overview/	This rule is triggered when a section's status on the Compliance Risk Score dashboard is changed manually.
Trend of Failed Administrative Actions	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	This trend stores a daily count of administrator user names and the number of their failed actions.
Configuration Changes	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	Collects hourly data using the Configuration Changes Trend Base query. Used by other queries to show configuration changes.
Software Detected	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	This trend stores events in which a piece of software is detected by a scanner.

Shutdown of Critical Machines	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	This trend stores long term aggregated information about shutdown of critical machines.
Count of Administrative Logins	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Stores a count of successful and unsuccessful administrative logins.
Failed Administrative Logins - Long Term Trend	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Stores long term information about failed administrative logins.
User Login Count	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Stores a daily count of on-administrative user login attempts.
Case History	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	This trend stores all case audit events.
Attacks and Suspicious Activities	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	This trend stores long term aggregated information about attacks and suspicious activity events.
Vulnerabilities	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Collects hourly data using the Vulnerabilities trend Base query.
DoS Attacks Trend	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	This trend stores long term aggregated information about DoS attack events.
Daily Trend of Anti-Virus Stopped or Paused Events	Trend	/All Trends/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 2 Flaw Remediation/	Stores all events when an Anti-Virus service is stopped or paused.

Appendix B: Asset and Zones Categories

Following is a list of all the categories used and the resources which use those categorizations.

Resource	Type	URI	Category URI
Access to Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Change Details in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Account Change Details in Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Change Details in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Change Details in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Account Change Details in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Account Change Details in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Account Creations in Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Account Creations in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Creations in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Creations in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Account Creations in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Account Deletions in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Deletions in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Deletions in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Account Deletions in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Account Modifications in Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Account Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Account Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Account Modifications in Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Asset Identification Report	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Assets Per Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/System Asset Categories/Criticality/
Assets by Application Type	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/
Assets by Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/
Assets by Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Assets by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Assets by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Assets in FIPS-199 Availability Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/
Assets in FIPS-199 Conditionality Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/
Assets in FIPS-199 Integrity Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/
Assets in NIST 800-53 High Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/High Impact/
Assets in NIST 800-53 Low Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Low Impact/
Assets in NIST 800-53 Moderate Impact Criticality	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Moderate Impact/
Assets in the Development Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Assets in the Operations Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/

Assets in the Production Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Assets in the Public-Facing Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Assets in the Test Network Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Assets in the Third Party Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Assets with E-Authentication Levels	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-63/E-Authenticaiton/
Attacker Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Attacker Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Attacker Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/
Attacker Asset is Production	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Attacker Asset is Remote	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Remote/
Attacker Asset is Third Party	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/

Attacker Asset is VOIP	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/VOIP/
Attacker Asset is Wireless	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Attacker Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Attacker Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/
Attacks and Suspicious Activities From a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Attacks and Suspicious Activities Targeting a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Attacks and Suspicious Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Attacks and Suspicious Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Attacks and Suspicious Activities from a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Attacks and Suspicious Activities from a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Attacks and Suspicious Activity Targeting Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/

Attacks and Suspicious Activity from Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Attacks and Suspicious Activity to and from Third Party Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Attacks and Suspicious Activity to and from Wireless Resources	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Attacks from Development Targeting Production	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Attacks from Development Targeting Production	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Attacks from Production Targeting Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Attacks from Production Targeting Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Attempted File Changes in Development originated from Other Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Blocked Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Blocked Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Blocked Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Blocked Firewall Traffic from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Blocked Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Blocked Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Blocked Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Blocked Firewall Traffic to Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Classification Level Traffic High to Low	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Classification Level Traffic Low to High	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Classification of Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Classified Machines	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/

Communication between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Communication between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Financial Assets and Public Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Financial Assets and Public Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Financial/
Communication between Financial Assets and Public Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Communication between Financial Assets and Public Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Communication between Production and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Production and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Communication between Production and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Production and Development Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Production and Development Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Communication between Sensitive Asset and Test Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Sensitive Asset and Test Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/System Asset Categories/Criticality/High/
Communication between Sensitive Asset and Test Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Communication between Sensitive Asset and Third Party Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Sensitive Asset and Third Party Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/System Asset Categories/Criticality/High/

Communication between Sensitive Asset and Third Party Domain	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Communication between Test and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Test and Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Communication between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Communication between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Third Party and Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Third Party and Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Third Party and Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Third Party and Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Communication between Third Party and Top Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Third Party and Top Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Third Party and Top Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Third Party and Top Secret Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/

Communication between Third Party and Unclassified Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communication between Third Party and Unclassified Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communication between Third Party and Unclassified Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Communication between Third Party and Unclassified Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/
Communications between Development and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communications between Development and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Communications between Development and Test	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Communications between Development and Test	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Communications between Test and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Communications between Test and Operations	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Configuration Changes in Third Party Machines	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA- 9 External System Services/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Configuration Modifications by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Configuration Modifications by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Configuration Modifications by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Configuration Modifications in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Configuration Modifications in Email Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Email/
Configuration Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Configuration Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/

Configuration Modifications in Personal Identifiable Information Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-29 Inventory of Personally Identifiable Information/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Configuration Modifications in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Configuration Modifications in Public-Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Configuration Modifications in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Configuration Modifications in Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/
Configuration Modifications in Wireless Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Count Assets per Zone and E-Authentication Level 3 or 4	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-63/E-Authenticaiton/
Count of Assets with E-Authentication Level 3 or 4 per Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-63/
Count of Assets with E-Authentication Level 3 or 4 per Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-63/E-Authenticaiton/Level 3/

Count of Assets with E-Authentication Level 3 or 4 per Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM- 5 System Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-63/E-Authenticaiton/Level 4/
Count of Attacks and Suspicious Activity Event Names in the Wireless Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Count of Attacks and Suspicious Activity Event Names in the Wireless Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Count of Attacks and Suspicious Activity Event Names on Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-18 Wireless Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Critical Asset Details on Development	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/System Asset Categories/Criticality/
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/System Asset Categories/Criticality/High/
Critical Asset Details on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/System Asset Categories/Criticality/Very High/

Critical Asset Details on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Critical Asset Details on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Critical Asset Details on Operations	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Critical Asset Details on Processing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Processing/
Critical Asset Details on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Critical Asset Details on Public-Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Critical Asset Details on Third-Party	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Critical Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Critical Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Critical Financial Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Financial/

Critical Machine Configuration Modifications at Unscheduled Time	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Critical Wireless Components	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Criticality of Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Criticality of Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/System Asset Categories/Criticality/
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Cross-Talk Between Network Domains - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Cross-Talk Between Network Domains - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Cross-Talk Between Test Environment and PII Asset	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Cross-Talk Between Test Environment and PII Asset	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Cross-Talk Between Test Environment and PII Asset	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Current Asset Count by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
DNS Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Domain Name Server/
Database Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database/
Development and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Email Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Email/
FIPS-199 Availability Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/

FIPS-199 Confidentiality Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/
FIPS-199 Integrity Criticality Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/
File Changes in Development	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
File Integrity Changes by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
File Integrity Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
File Integrity Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Financial assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Financial/
Firewall Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/Firewall/
Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Firewall Traffic from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Firewall Traffic to Assets - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Firewall Traffic to Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Firewall Traffic to Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
High to Low Classified Asset Communication	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/

Higher to Lower Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/
Human Resources Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Human Resources/
Information System Failures	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	/All Asset Categories/System Asset Categories/Criticality/High/
Information System Failures	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 7 Continuous Monitoring/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Inter-Domain Traffic	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Internal Attackers	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/
Internal Inter-Domain Traffic	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Internal Inter-Domain Traffic by Attacker Domain	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Internal Inter-Domain Traffic by Target Domain	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Internal Targets	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected/

Last 10 Asset Creations	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Asset Deletions	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Asset Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Communications between Operations and Development Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Internal Inter-Domain Traffic	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Resource Exhaustion Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Security Log is Full Events	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Last 10 Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Successful Administrative Logouts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Successful Administrative Logouts	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 10 Traffic to Development from other Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 10 Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/

Last 20 Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 20 Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Last 20 Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Last 20 Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Low to High Classified Asset Communication	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/
Lower to Higher Classification Level	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/

Machines Conducting Policy Breaches	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/System Asset Categories/Criticality/
Machines Conducting Policy Violations	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/System Asset Categories/Criticality/
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database/
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Domain Name Server/
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Web Server/
Multiple Policy Violations Against Assets Categorized with the Same Network Domains	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
NIST 800-53 High Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/High Impact/
NIST 800-53 Low Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Low Impact/
NIST 800-53 Moderate Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Low Impact/

NIST 800-53 Moderate Impact Assets Overview	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Moderate Impact/
Network Device Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network/
Network Device Configuration Modifications at Unscheduled Time	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Maintenance (MA)/MA- 2 Controlled Maintenance/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network/
Network IDS Configuration Modifications	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Security Devices/NIDS/
New Personal Identifiable Information Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-29 Inventory of Personally Identifiable Information/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
New Systems by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
New Systems by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
New Systems by Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
New Systems on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
New Systems on Public-Facing Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/

New Systems on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
New Systems on Third-Party Accessible Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/
New Wireless Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Non-Operating System Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Operating System/
Number of New Systems by FIPS-199 Availability Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/
Number of New Systems by FIPS-199 Confidentiality Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/
Number of New Systems by FIPS-199 Confidentiality Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/
Number of New Systems by FIPS-199 Integrity Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/
Number of New Systems with FIPS-199 or NIST 800-53 High Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/High Impact/
Number of New Systems with FIPS-199 or NIST 800-53 High Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/High/

Number of New Systems with FIPS-199 or NIST 800-53 High Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/High/
Number of New Systems with FIPS-199 or NIST 800-53 High Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/High/
Number of New Systems with FIPS-199 or NIST 800-53 Low Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Low Impact/
Number of New Systems with FIPS-199 or NIST 800-53 Low Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/Low/
Number of New Systems with FIPS-199 or NIST 800-53 Low Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/Low/
Number of New Systems with FIPS-199 or NIST 800-53 Low Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/Low/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/Moderate Impact/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/High/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/Moderate/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/High/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/Moderate/

Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/High/
Number of New Systems with FIPS-199 or NIST 800-53 Moderate Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/Moderate/
Number of New Systems with FIPS-199 or NIST800-53 by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Number of New Systems with FIPS-199 or NIST800-53 by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/
Number of New Systems with FIPS-199 or NIST800-53 by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 6 Configuration Settings/	/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/
Operating System Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Operating System/
Operating System Assets by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operating System Assets by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Operating System/
Operating System Assets by Network Zone	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Operating System/

Operating System Assets by Operating System	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/Site Asset Categories/Operating System/
Operating Systems Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operating Systems Configuration Modifications by Host Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operating Systems Configuration Modifications by Process Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operating Systems Configuration Modifications by User Name	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operations and Development Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Operations and Test Cross-Talk	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Organizational Information Leaks on Databases	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database/
Organizational Information Leaks on Legal Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Legal/

Organizational Information Leaks on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Organizational Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Organizational Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Organizational Information Leaks on Processing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Processing/
Organizational Information Leaks on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Organizational Information Leaks on Public-Facing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Organizational Information Leaks on Third-Party Accessible Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/
Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Personal Information Leaks on Commerce Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Commerce/
Personal Information Leaks on Databases	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Database/

Personal Information Leaks on Electronic PII	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Personal Information Leaks on Email Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Email/
Personal Information Leaks on Financial Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Financial/
Personal Information Leaks on HR Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Human Resources/
Personal Information Leaks on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Personal Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Personal Information Leaks on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-13 Monitoring for Information Disclosure/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Personal Information Leaks on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Policy Violations Originated from Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Policy Violations Originated from Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Policy Violations Originated from Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Partner/
Policy Violations Originated from Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Policy Violations on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Policy Violations on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Policy Violations on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Planning (PL)/PL- 1 Planning Policy and Procedures/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Partner/
Policy Violations on Third Party Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Potential Insider Threat Campaign Against the organization	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-12 Insider Threat Program/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Reconnaissance Activities From a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Reconnaissance Activities From a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Reconnaissance Activities From a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Reconnaissance Activities Targeting Electronic PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/

Reconnaissance Activities Targeting Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Reconnaissance Activities Targeting Public-Facing	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Reconnaissance Activities Targeting a Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Reconnaissance Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Reconnaissance Activities Targeting a Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Resource Exhaustion Detected - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Resource Exhaustion Detected on Critical Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Resource Exhaustion Detected on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Resource Exhaustion Detected on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Resource Exhaustion Detected on Processing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Processing/
Resource Exhaustion Detected on Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/

Resource Exhaustion Detected on Public Facing Systems	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Resource Exhaustion Detected on Third Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU- 4 Audit Storage Capacity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/
Shared Machines among Test Environment and Personal Identifiable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Shared Machines among Test Environment and Personal Identifiable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Shared Machines among Test Environment and Personal Identifiable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Shared Machines among Test, Development and Operation	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Shared Machines among Test, Development and Operation	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Shared Machines among Test, Development and Operation	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Shared Machines among Test, Development and Operation	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Shutdown of Critical Machines on Development Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Shutdown of Critical Machines on Email Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Email/
Shutdown of Critical Machines on Financial Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Financial/
Shutdown of Critical Machines on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Shutdown of Critical Machines on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Shutdown of Critical Machines on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Shutdown of Critical Machines on Operations Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
Shutdown of Critical Machines on Processing Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Processing/
Shutdown of Critical Machines on Production Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Shutdown of Critical Machines on Public-Facing Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Shutdown of Critical Machines on Third-Party Domain	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/

Shutdown of Critical Wireless Components	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 - Contingency Plan/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Software Changes by Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Software Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Software Changes by Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Software Detected - Trend Base	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Successful Administrative Logins between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Successful Administrative Logins between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Administrative Logins between 2 Network Domains	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Successful Administrative Logins between 2 Network Domains	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between Development and Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Administrative Logins between Development and Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Successful Administrative Logins between Development and Production	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 9 Internal System Connections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between Test Environment and PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Administrative Logins between Test Environment and PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Successful Administrative Logins between Test Environment and PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/PM-26 Minimization of Personally Identifiable Information Used in Testing, Training, and Research/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Successful Administrative Logins between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between Third Party and Development Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Successful Administrative Logins between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Administrative Logins between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Successful Administrative Logins between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Successful Administrative Logins between Third Party and Production Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Assessment, Authorization, and Monitoring (CA)/CA- 3 System Interconnections/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Successful Logins to Intellectual Property Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Intellectual Property/
Successful Logins to Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Successful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Successful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Successful Logins to Patient Medical Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PHI/
Successful Logins to Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Successful Removal of Access Rights - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Removal of Access Rights - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Removal of Access Rights in Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Removal of Access Rights in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Removal of Access Rights in Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Successful Removal of Access Rights in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Successful Removal of Access Rights in Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 5 Access Restrictions for Change/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/

Suspicious Activity on Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Target Asset Categorized in Network Domains	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Target Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Target Asset is Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/
Target Asset is Critical	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/System Asset Categories/Criticality/High/
Target Asset is Critical	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Target Asset is Database	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight System Administration/Databases/
Target Asset is Database	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database/
Target Asset is Development	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Target Asset is High Impact System	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/NIST 800-53/High Impact/
Target Asset is PII	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Target Asset is Production	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/

Target Asset is Publcing Facing	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Target Asset is Third Party	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party/
Target Asset is VOIP	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/VOIP/
Target Asset is Wireless	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Target Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret/
Target Asset is not Classified	Filter	/All Filters/ArcSight Solutions/FISMA/General Filters/Assets/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret/
Third-Party Access	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Administrative Users with Successful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Administrative Users with Successful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Administrative Users with Unsuccessful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/

Top 10 Administrative Users with Unsuccessful Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Asset Network Domains with Account Creation Deletion and Modification	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 2 Account Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Assets with Critical Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Assets with Critical Vulnerabilities	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Communications between Operations and Development Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 5 Separation of Duties/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Devices with Configuration Modifications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Hosts with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/

Top 10 Hosts with Successful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Successful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Hosts with Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Successful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Hosts with Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Unsuccessful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Hosts with Unsuccessful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Unsuccessful Administrative Logins from Third Party systems	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC-20 Use of External Systems/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/

Top 10 Hosts with Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Unsuccessful Logins to Development	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Hosts with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Hosts with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Network Domains with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Network Domains with Successful Administrative Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Network Domains with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Network Domains with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/

Top 10 Traffic to Development from other Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Users with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top 10 Users with Unsuccessful User Logins	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/
Top 10 Vulnerabilities	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/
Top 10 Vulnerable Assets	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Regulation/FISMA/
Top 10 Vulnerable Assets on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 7 - Boundary Protection/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Assets on Network Domain - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Top 10 Vulnerable Assets on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Assets on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Top 10 Vulnerable Assets on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Assets on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Top 10 Vulnerable Critical Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Critical Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Top 10 Vulnerable PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Top 10 Vulnerable Public Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Top 10 Vulnerable Public Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Top 10 Vulnerable Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Top 10 Vulnerable Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/
Top Configuration Modifications by Network Domains	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Top Internal Inter-Domain Communications	DataMonitor	/All Data Monitors/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Traffic Between Network Domains	ActiveChannel	/All Active Channels/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Traffic Between Network Domains	FieldSet	/All Field Sets/ArcSight Solutions/FISMA/NIST 800-53/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Traffic from Dark Address Space	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Address Spaces/Dark/
Traffic from Others to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Traffic from Others to Development	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/System and Service Acquisition (SA)/SA-10 Developer Configuration Management/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Traffic to Dark Address Space	Filter	/All Filters/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 4 Information Flow Enforcement/	/All Asset Categories/Site Asset Categories/Address Spaces/Dark/
Unsuccessful Logins to Intellectual Property Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Intellectual Property/

Unsuccessful Logins to Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Unsuccessful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Unsuccessful Logins to Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Unsuccessful Logins to Patient Medical Records	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Media Protection (MP)/MP- 2 Media Access/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PHI/
Unsuccessful Logins to Personal Identification Information Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Unsuccessful Operating Systems Configuration Modifications	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 3 Configuration Change Control/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
VOIP Application Detected	Rule	/All Rules/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/VOIP/
VOIP Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/VOIP/
Vulnerabilities Summary on Critical Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/System Asset Categories/Criticality/Very High/
Vulnerabilities Summary on Development Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

Vulnerabilities Summary on Network Domain	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Vulnerabilities Summary on Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/
Vulnerabilities Summary on Network Domain	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Vulnerabilities Summary on PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Privacy Authorization (PA)/PA- 3 Purpose Specification/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Vulnerabilities Summary on PII Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Electronic PII/
Vulnerabilities Summary on Production Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Vulnerabilities Summary on Public Facing Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Vulnerabilities Summary on Test Environment	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 4 Security and Privacy Impact Analysis/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/
Vulnerabilities Summary on Third-Party Accessible Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third-Party Accessible Assets/

Web Application Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Web Server/
Wireless Assets	FocusedReport	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/CM- 8 System Component Inventory/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless/
Zones Per Criticality	Query	/All Queries/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP- 2 Contingency Plan/	/All Asset Categories/System Asset Categories/Criticality/

Appendix C: Resources Requiring Enabled Trends

Below is the list of end user resources that require enabling trends to show data:

Resource	Type	URI	Required Trends
Trend of Failed Administrative Actions per Product	Report	All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	Trend of Failed Administrative Actions
Trend of Failed Administrative Actions	Report	All Reports/ArcSight Solutions/FISMA/NIST 800-53/Audit and Accountability (AU)/AU-12 Audit Generation/	Trend of Failed Administrative Actions
Weekly Report - Configuration Modifications by User Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 3 Configuration Change Control/	Configuration Changes
Weekly Report - Configuration Modifications by Host Name - Template	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 3 Configuration Change Control/	Configuration Changes
Weekly Trend - Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 3 Configuration Change Control/	Configuration Changes
Software Summary by Network Domain in Last 2 Weeks	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 8 System Component Inventory /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/ PM- 5 System Inventory	Software Detected
Software Products on Specific Asset - Template	Report	/ All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 8 System Component Inventory /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/ PM- 5 System Inventory	Software Detected
Software Summary in Last 2 Weeks	Report	/ All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 8 System Component Inventory /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/ PM- 5 System Inventory	Software Detected

Software Summary by Zone in Last 2 Weeks	Report	/ All Reports/ArcSight Solutions/FISMA/NIST 800-53/Configuration Management (CM)/ CM- 8 System Component Inventory /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Program Management (PM)/ PM- 5 System Inventory	Software Detected
Weekly Trend - Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Contingency Planning (CP)/CP - 2 Contingency Plan	Shutdown of Critical Machines
Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Count of Administrative Logins
Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	Count of Administrative Logins Failed Administrative Logins - Long Term Trend
Number of Successful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	User Login Count
Number of Unsuccessful User Logins over the Past Week	Report	/ All Reports/ArcSight Solutions/FISMA/NIST 800-53/Identification and Authentication (IA)/IA- 2 Identification and Authentication (Organizational Users)/	User Login Count
Average Time to Resolution - By Case Severity	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	Case History
Average Time to Resolution - By Day	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	Case History
Average Time to Resolution - By User	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 5 Incident Monitoring/	Case History
Weekly Report - Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/IR- 6 Incident Reporting	Attacks and Suspicious Activities
Weekly Trend - Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Incident Response (IR)/ IR- 6 Incident Reporting	Attacks and Suspicious Activities

Weekly Report - XSRF Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/ /All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	Vulnerabilities
Weekly Report- CVSS Score Greater than or Equal to 8 Overview	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Vulnerabilities
Weekly Report - XSS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/ /All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	Vulnerabilities
Weekly Report - Vulnerability Summary	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Vulnerabilities
Weekly Report - SQL Injection Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/ /All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-10 Information Input Validation/	Vulnerabilities
Weekly Report - Vulnerabilities by Host Name	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Vulnerabilities
Weekly Report - Insecure Cryptographic Storage	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-28 Protection of Information at Rest/	Vulnerabilities
Weekly Report - VOIP Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-19 Voice Over Internet Protocol	Vulnerabilities
Weekly Report - Cryptographic Hash Algorithm Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - Cryptographic Public Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities

Weekly Report - Vulnerabilities by CVE ID	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Vulnerabilities
Weekly Report - ASLR or Data Execution Prevention Bypass Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI-16 Memory Protection/	Vulnerabilities
Weekly Report - SSL|TLS Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - Overflow Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/Risk Assessment (RA)/RA- 5 Vulnerability Scanning/	Vulnerabilities
Weekly Report - Cryptographic Symmetric Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - VPN Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - Cryptographic Weak Protocol Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - SSH Vulnerabilities	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC-13 Cryptographic Protection/	Vulnerabilities
Weekly Report - BIOS Flaws	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/SI- 7 Software,Firmaware, and Information Integrity/	Vulnerabilities
Weekly Trend - DoS Attacks	Report	/All Report/ArcSight Solutions/FISMA/NIST 800-53/System and Communications Protection (SC)/SC- 5 Denial of Service Protection/	DoS Attacks Trend
Weekly Report- Anti-Virus Stopped or Paused	Report	/All Reports/ArcSight Solutions/FISMA/NIST 800-53/System and Information Integrity (SI)/ SI- 2 Flaw Remediation	Daily Trend of Anti-Virus Stopped or Paused Events

Appendix D: Compare, Backup and Uninstall Package

This chapter provides instructions for the backup and uninstall of the Compliance Insight Package for FISMA (CIP for FISMA). This appendix is not part of the initial configuration and is provided if you want to generate a list of resource changes, back up the solution package or uninstall the CIP for FISMA at a later date.

Generate a List of Resource Changes

Before backing up a solution package, you may want to generate a list of resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified or deleted resources are reported.

Note: Every time a package is exported, the change history is reset.

To generate a list of resource changes:

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the **Packages** tab of the Navigator panel, navigate to the solution group.

   For CIP for FISMA, navigate to `ArcSight Solutions/FISMA 6.0`.
3. Right-click the solution package () and select **Compare Archive with Current Package Contents.**

   In the Viewer panel, a list of resources associated with the package are displayed. In the right column called `Change Since Archive`, any changes with the resource since the last export are displayed, either `Added`, `Modified`, or `Removed`.
4. Optional—For future reference, you can copy and paste the cells from the list into a spreadsheet.

Back Up the Solution Package

ArcSight recommends that you have a backup of the current state before making content changes or installing/uninstalling solution packages. Before backing up a solution, you may want to get a list of changed resources. You may want to back up only those resources that have been modified or added. For detailed instructions, see "Generate a List of Resource Changes" above.

You can back up the solution content to a package bundle file that ends in the `.arb` extension as described in the process below.

To back up a solution package:

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the Packages tab of the Navigator panel, navigate to the solution group.

   For CIP for FISMA, navigate to `ArcSight Solutions/FISMA 6.0`.
3. Right-click the solution package () and select **Export Package(s) to Bundle**.

   The Package Bundle Export dialog displays.
4. In the Package Bundle Export dialog, browse for a directory location, specify a file name and click **Next**.

   The Progress tab of the Export Packages dialog displays the progress of the export.
5. When the export is finished, click **OK**.

   The resources are saved into the package bundle file that ends with the `.arb` extension. You can restore the contents of this package at a later time by importing this package bundle file.

Uninstall the CIP for FISMA

Before uninstalling the CIP for FISMA, backup all the packages () for all the solutions currently installed on the ESM Manager.

For example, if the CIP for FISMA and the PCI solution are both installed on the same ESM Manager, export the package(s) for each solution before uninstalling either solution. Back up the PCI package into a package bundle (ARB) file and then back up the CIP for FISMA into a different package bundle (ARB) file before uninstall either solution. For detailed instructions, see "Back Up the Solution Package" on the previous page. You may also want to generate a list of changes before the uninstall. For detailed instructions, see "Generate a List of Resource Changes" on the previous page.

To uninstall the CIP for FISMA:

1. Log into the ArcSight Console as ArcSight Administrator.
2. Click the Packages tab in the Navigator panel.
3. In the Packages tab of the Navigator panel, navigate to `ArcSight Solutions/FISMA 6.0`.
4. Right-click the `FISMA 6.0` package () and select **Uninstall Package**.
5. In the Uninstall Packages dialog, click **OK**.

   The progress of the uninstall displays in the `Progress` tab of the Uninstalling Packages dialog.
6. When the uninstall is finished, click **OK**.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (ESM CIP for FISMA 6.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!