Micro Focus Security

ArcSight ESM

CIP for IT Gov

Software Version: 5.0

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

Contents

Chapter 1: Solution for ITGov CIP Overview and Architecture

Organizations in many industries are subject to regulations that require adherence to certain practices to ensure business continuity and information security. For example, Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and Basel II require that affected organizations use a framework of controls to implement policies, procedures, and physical and technical safeguards to protect the business and its assets. Because each organization's business practices are unique, regulations typically do not address implementation details.

The ISO Family of Standards

Regulatory compliance can best be enforced and demonstrated by the use of a cohesive framework, such as the code of practice for information security management, or ISO/IEC 27002. This standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and covers the controls and guidelines a company should implement according to best practices in IT security.

ISO 27002 Standard

ISO27002 is a comprehensive set of controls comprising best practices in information security and provides guidelines on how to set-up and maintain a security program.

IS27002 is based on the British standard BS 7799, which adopted by ISO/IEC and revisited in 2005 and renumbered in 2007 to ISO27002 (referred as ISO27002:2005)

In 2013 the standard re-visited again by providing new controls, removing un-needed controls to address the up to date threats and attacks (referred as ISO27002:2013)

The standard covers a set of 18 security categories. Sections 1 through 4 of the standard cover introductory material; the remaining sections include:

- Section 5: Information Security Policies
- Section 6: Organization of Information Security
- Section 7: Human Resource Security
- Section 8: Asset Management
- Section 9: Access Control
- Section 10: Cryptography

- Section 11: Physical and environmental security
- Section 12: Operation Security
- Section 13: Communication Security
- Section 14: System acquisition, development and maintenance
- Section 15: Supplier relationships
- Section 16: Information Security Incident Management
- Section 17: Information Security Aspects of business continuity management
- Section 18: Compliance

Compliance Insight Package for IT Governance

The Compliance Insight Package for IT Governance helps you implement your organization's security program and demonstrate regulatory compliance based on the ISO/IEC 27002 standard. It is a layered solution that leverages the more encompassing business policy focus of ISO/IEC 27002:2013.

CIP for IT Governance addresses these 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:** The ISO/IEC 27002 and NIST 800-53 standards are internationally recognized frameworks for information security best practices. By delivering content based directly on ISO/IEC 27002 the CIP for IT Governance can be used to help implement, monitor and manage a best practices approach to information security management.
- **Automation of Monitoring-IT control:** CIP for IT Governance follows and adapts to changes in the IT environment. More than 60 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 which allows analysts to quickly analyze situations.
- **Vulnerabilities and Configuration Changes Monitoring:** Tracking vulnerabilities and configuration changes.

Solution Architecture

The *Solution for ITGov CIP* provides ArcSight ESM resources that can assist with compliance to the ITGov CIP Standards. Resources that help address a specific IT Governance CIP Standard are stored in the corresponding directory. For example, the Privileged Account Change Details report is provided to

assist in compliance with ISO 9, and is stored in the corresponding group, as shown in the following figure.

In addition to the resources supplied to help address specific ISO sections, there is a common set of filters and active lists that support the entire solution. These common resources are described in "Solution Installation and Configuration" on page 9 These resources require configuration to tailor the content for your environment, such as privileged account names or the working hours in your organization.

For all resources covered by Solution for ITGov CIP, see "Resource Reference" on page 41.

Overview Dashboards

Overview dashboards are provided that summarize the compliance state determined by correlation rules for each ISO section. The overview dashboards are available from the IT Governance/Overview group as shown in the following figure.

Each dashboard presents an event graph to show the relationships of the non-compliant systems with other systems on the network; a list of the last 20 triggered rules; a pie chart that breaks down the percentage of each triggered rule; and a bar chart that shows the top 20 targets of the triggered rules.

The following figure shows the ISO 9 Overview dashboard.

The Compliance Risk Score Overview dashboard is a centralized heads-up display that shows the current state of compliance for each of the ISO Standards by displaying the results of Compliance Risk Score Overview last-state data monitor. The dashboard summarizes your environment's overall state of compliance with the ISO Sections as determined by correlation rules triggered for each family.

Notify, Investigate, Analyze, and Remediate

Once a security or compliance-related activity is identified, *Compliance Insight Package for ITGov v5.0* 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. You can configure the rules included in Solution for ITGov CIP to activate your notification hierarchy in case of

certain threats. You can configure this hierarchy to notify the right groups in the right situations. For more information, see "Configure Notifications " on page 38.

Cases

 Cases are ArcSight's built-in trouble-ticket system. When certain compliance-related conditions occur, the Solution for ITGov CIP can be configured to open a case to track an issue so it can be investigated and properly remediated. For more information, see "Configure Cases" on page 34.

Chapter 2: Solution Installation and Configuration

This chapter contains information on installing and configuring the *Compliance Insight Package for ITGov v5.0* (Solution for ITGov CIP).

Prepare for Installation

Before installing Solution for ITGov CIP, complete the following preparation tasks:

1. "Prepare Environment" below
2. "Verify Environment" below
3. "Verify Supported Platforms" on the next page

Prepare Environment

Before installing, prepare your environment for the Solution for ITGov CIP:

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

   Note: RFC 1918 addresses(10.x.x.x, 192.168.x.x, 172.16-31.x.x) are automatically categorized as protected because their zones already are categorized as protected.

Verify Environment

Verify that your system has the ArcSight ESM Console connected to an ArcSight ESM Manager with this ESM product version installed and meets the prerequisite requirements.

Note: The Solution for ITGov CIP is a self-contained solution that does not rely on any other ArcSight solution. You can install the Solution for ITGov CIP with other solutions on the same Manager. Before installing new solutions, ArcSight recommends that you back up any existing

solutions installed on the ESM Manager. For detailed instructions, see "Compare, Backup, and Uninstall Packages" on page 226.

Updating from ITGov 4.0 SP2 to ITGov (Version 5.0) requires :

1. Back up the old solution installed on the Manager, see "Compare, Backup, and Uninstall Packages" on page 226.
2. Uninstall ITGov 4.0 SP2.
3. Install ITGov (Version 5.0)

Verify Supported Platforms

The Solution for ITGov CIP operates on all supported Micro Focus ESM platforms 6.9.1 or higher, and is installed through the ArcSight ESM Console using the package import feature.

Install Solution for ITGov CIP

The solution is supplied in a single Micro Focus package bundle file called ArcSight-ComplianceInsightPackage-ITGov.5.0<nnnn>.arb, where <nnnn> is the 4 character build number.

To install the Solution for ITGov CIP package:

1. Using the log-in credentials supplied to you by ArcSight, download the Solution for ITGov CIP package bundle from the Micro Focus software download site to the machine where you plan to launch the ArcSight ESM Console:

   `ArcSight-ComplianceInsightPackage-IT Governance.5.0.<nnnn>.arb`

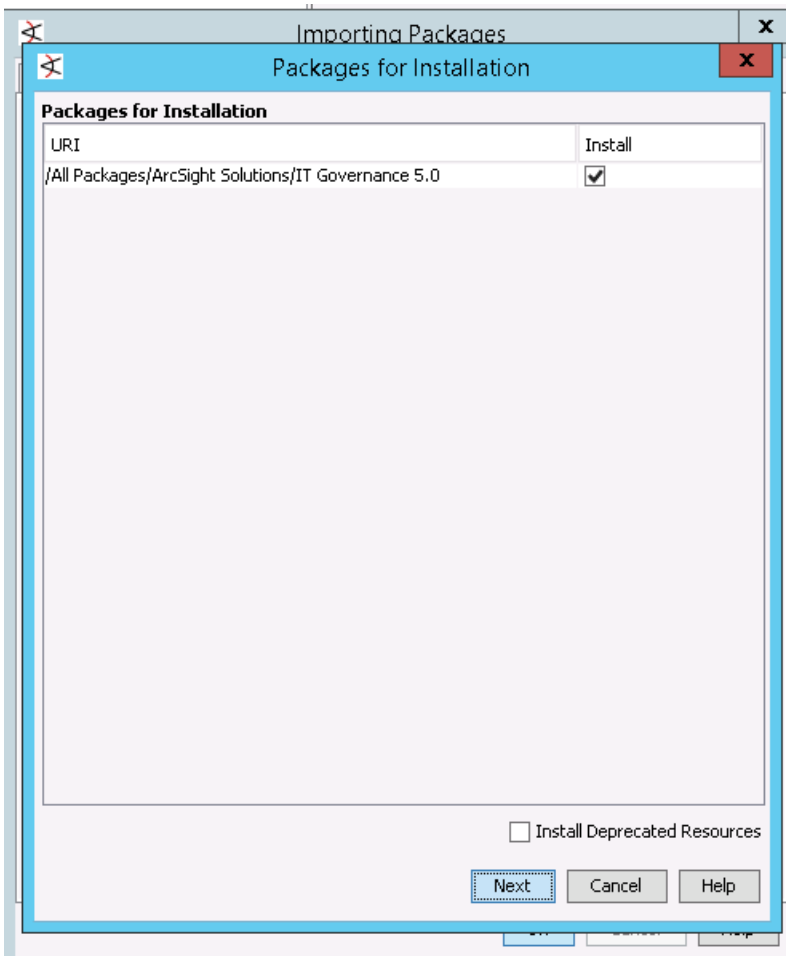
   Where <nnnn> is the 4 character build number. (The exact build number is specified in the *ArcSight Compliance Insight Package for ITGov v5.0 Release Notes*.)

   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 ESM Console as a user with administrative privileges.
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**.

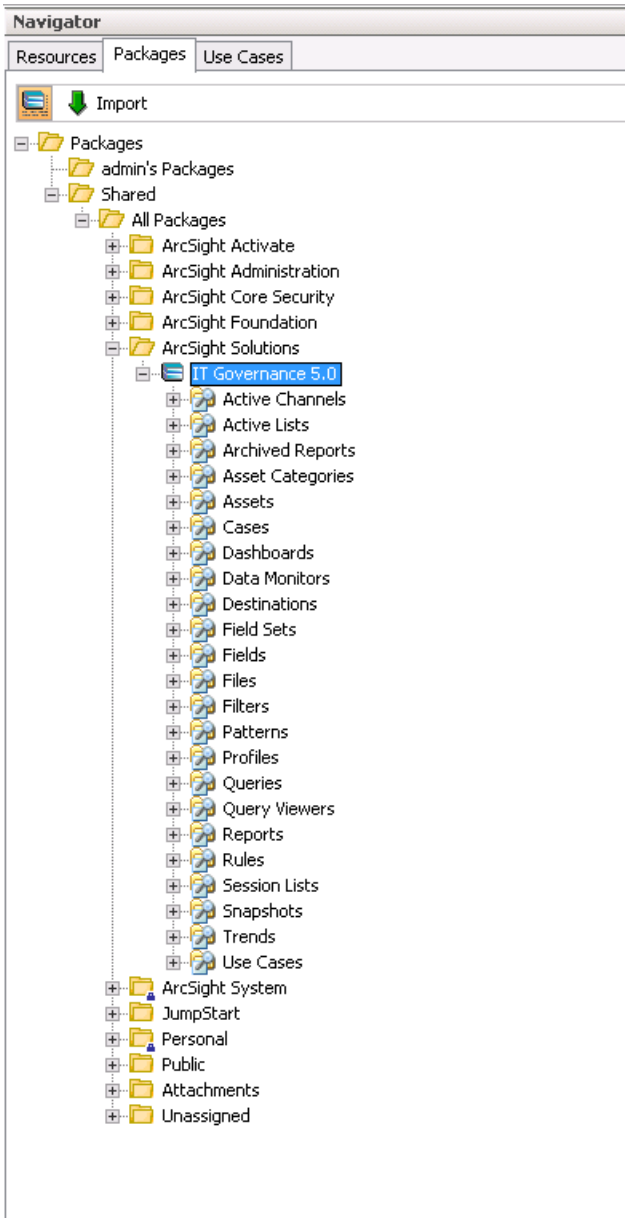
   The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

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



6. Leave the ITGov 5.0 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/IT Governance 5.0` group.



Assign User Permissions

By default, users in the `Default` user group can view Solution for ITGov CIP 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

To assign user permissions:

1. Log into the ArcSight ESM Console as a user with administrative privileges.
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/ITGov`.
   b. Right-click the **ITGov** 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 Solution for ITGov CIP resources and click **OK**.

Configure Solution for ITGov CIP

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

This section contains the instructions required to enable content for the *Solution for ITGov CIP* and contains the following topics:

- "Configure Notifications " on page 38
- "Configure Additional Resources" on page 39

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

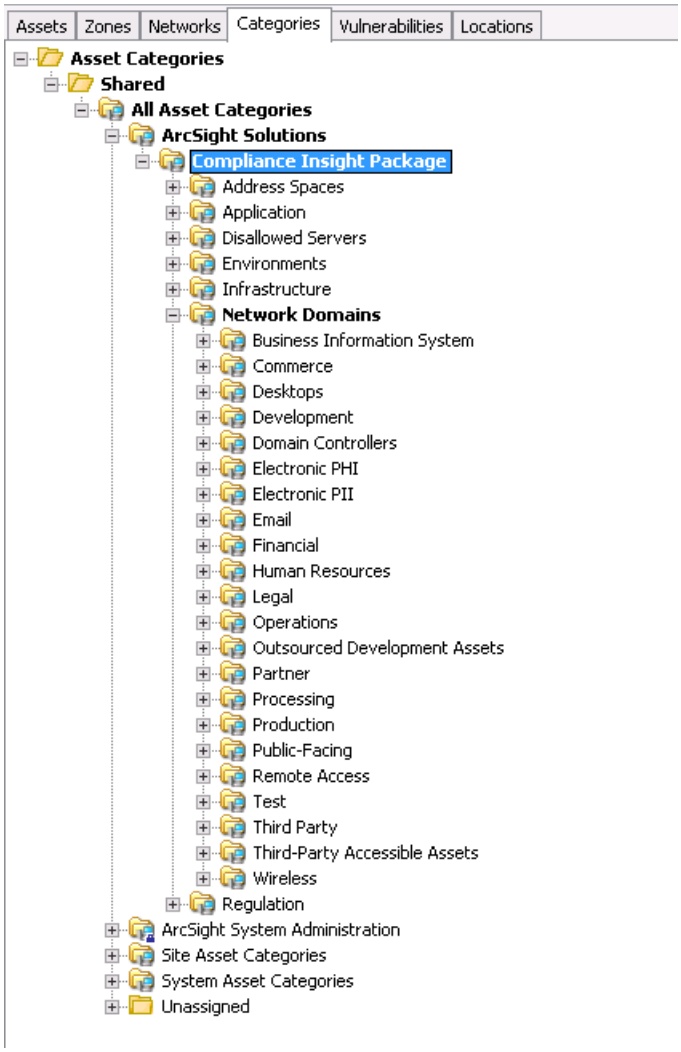
Model Assets (Assign Asset Categories)

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

- Some of the *Solution for ITGov CIP* 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 *Solution for ITGov CIP*.

CIP for IT Governance Categorization

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



Categorizing Assets and Zones

IT Governance solution relies on ArcSight asset and zone categorization to define your environment. Certain content does not display unless assets or zones are categorized.

Below a list of all the asset and zone categorization used and the filters which use those categorizations.

	Asset Categorizing	Zone Categorization
Attacker Asset Categorized in Network Domains Target Asset Categorized in Network Domains	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/	
Attacker Asset is Third Party Target Asset is Third Party And All the Filters of ISO 15 Section	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Third Party

	Asset Categorizing	Zone Categorization
Internal Attacker Internal Target Internal Connection Inbound Events Outbound Events Outbound Internet Activity Successful Non Secure Remote Access Non Secure Remote Access Attempts New Hire Based Internet Outbound Activity Disallowed Ports Access from Internal Hosts Disallowed Ports Access to Internal Hosts Internal Inter-Domain Traffic External to Internal Traffic Internal to External Traffic	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Address Spaces/Protected

	Asset Categorizing	Zone Categorization
Attacker Asset is Development Target Asset is Development Traffic from Others to Development Successful Logins to Development Unsuccessful Logins to Development	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/
Attacker Asset is Domain Server Target Asset is Domain Server	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Domain Name Server/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Domain Name Server/
Attacker Asset is Production Target Asset is Production	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Production/
Attacker Asset is Web Server Target Asset is Web Server	All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Web Server	All Asset Categories/ArcSight Solutions/Compliance Insight Package/Application/Type/Web Server
Attacker Asset is Wireless Target Asset is Wireless Wireless Malicious Traffic Detected	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Wireless

	Asset Categorizing	Zone Categorization
Target Asset is Critical	/All Asset Categories/System Asset Categories/Criticality/Very High	/All Asset Categories/System Asset Categories/Criticality/Very High
Removable Media Detected on Highly Critical Machine	/All Asset Categories/System Asset Categories/Criticality/High	/All Asset Categories/System Asset Categories/Criticality/High
Startup and Shutdown of Highly Critical Assets		
System Shutdown of Highly Critical Assets		
Target Asset is Database	/All Asset Categories/ArcSight System Administration/Databases	/All Asset Categories/ArcSight System Administration/Databases
	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Service/Database
Target Asset is Public Facing	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing/
Communications between Development and Operations	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/	"/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Operations/
	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/

	Asset Categorizing	Zone Categorization
Communications between Development and Test	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test/	/All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Development/ /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Test
Traffic from Higher to Lower Classification Level Traffic from Lower to Higher Classification Level	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/ /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/ /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Unclassified/ All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/ /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Secret /All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/Top Secret

	Asset Categorizing	Zone Categorization
Traffic to and from Classified Machines	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Classification/
Traffic from Dark Address Space Traffic to Dark Address Space	All Asset Categories/Site Asset Categories/Address Spaces/Dark/	All Asset Categories/Site Asset Categories/Address Spaces/Dark/

	Asset Categorizing	Zone Categorization
IM Traffic	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Yahoo IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Yahoo IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Google IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/Google IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/AOL IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/AOL IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/ICQ	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/ICQ
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/IRC	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/IRC
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/MSN IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/MSN IM
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/KIK	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/KIK
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SNAPCHAT	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SNAPCHAT
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SKYPE	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/SKYPE
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/FACEBOOK IM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/FACEBOOK IM

	Asset Categorizing	Zone Categorization
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/WhatsApp	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/WhatsApp
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/VIBER	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/VIBER
	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/TELEGRAM	/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/TELEGRAM

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 Compliance Insight Package 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 for IT Governance, see the ArcSight Asset Import File SmartConnector Configuration Guide.

Configure Active Lists

Solution for ITGov CIP contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by Micro Focus resources that use conditions, such as filters, rules, and reports.

You can populate the *Solution for ITGov CIP* active lists using any of the following processes:

- Add entries to active lists, one-by-one, using the Active List editor in the ArcSight ESM Console. For detailed instructions, see "Configure Active Lists Using Console Active List Editor" on page 27. 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 28. This method can be used to populate active lists with one, two, or more columns.

Some active lists are intended to be populated by rules and other required configurations. The following table defines all the active lists for the *Solution for ITGov CIP* and their configuration requirements.

Active List	Description	Configuration Required	Expected Input Per Entry
Active Accounts	This active list stores user names who have successfully logged in within the last 30 days.	No	
Administrative Accounts List	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".	Yes	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.	Yes	Connection type and port number Where Connection type could be: Inbound, outbound or internal
Audit Log Cleared	This active list should be populated only by the rule Audit Log Cleared. It logs every time an audit log is cleared.	No	
Badged In	This list contains information about employees who are badged in.	No	
Badged Out	This active list contains the computer accounts of badged out employees.	No	

Active List	Description	Configuration Required	Expected Input Per Entry
Badges to Accounts	This list contains the computer account and employee type for every physical device badge.	Yes	Badge ID, primary computer account for the badgeholder, and the employee type (in lowercase). Specifically, ensure that contractors are identified with the word "Contractor" (case insensitive) in the `employee type` field.
Compliance Score	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.	No	
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.	Yes	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.	Yes	Connection type and port number Where Connection type could be: inbound, outbound or internal
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.	Yes	User Name, in lowercase. **This list should be maintained on a regular basis.**
Insecure Ports	This active list includes ports related to unencrypted and thus insecure communication services.	Yes	Port number
Insecure Processes	This active list includes the names of processes that provide unencrypted and thus insecure communications.	Yes	Process name, in lowercase

Active List	Description	Configuration Required	Expected Input Per Entry
Instant Messaging Domains	This active list contains all the DNS domains for public instant messaging servers. This list is used to detect when outbound traffic to these domains is detected, signifying a possible information leak. Note: All the domain names must be in lowercase.	Yes	Domain name of popular or known instant messaging server in lowercase
Internal Systems with Insecure Services	This list stores all internal systems with insecure services detected, populated only by the rule “Internal Insecure Service Provider Detected."	No	
Internet Ports	This active list includes ports that are used for monitoring internet (Web traffic) communication. By default, it includes ports 80 and 443.	Yes	Port number
Monitored Accounts	This active list is used to maintain user accounts to be monitored.	Yes	Usernames in lowercase
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.	Yes	User Name, in lowercase. **This list should be maintained on a regular basis.**
Password Changes	This active is updated with the user and product information when a successful password change occurs.	No	
Peer to Peer Ports	This active list contains the ports involved in peer-to-peer traffic	Yes	Should be maintained on a regular basis.
Stale Accounts	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.	No	
Suspicious Activities by New Hires	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.	No	
Test and Custom Accounts	This active list 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.	Yes	Usernames in lowercase
Unsecured Password Signature	This active list contains unsecured password signatures.	Yes	

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 ESM Console.

1. In the Navigator panel, go to Lists and navigate to `ArcSight/Solutions/IT Governance`.
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. Do not include columns for Creation Time, Modification Time, or Count in the CSV file.

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

   A file browser displays.
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
- "Intellectual Property Download Filter" below
- "Limit Regulation Filter" below

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 ESM 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 shown in the following figure.

Intellectual Property Download Filter

The `Intellectual Property Download` filter finds events that involve the possible illegal download of intellectual property. By default, this filter is set to find a Snort signature that indicates video or audio download. Add the signatures for the content monitoring device(s) or NIDS you use that indicate intellectual property downloads, such as video streams, images, audio files, or possibly illegal intellectual property or copyrighted material.

Limit Regulation Filter

The Limit Regulation filter limits event processing to only those events addressed by the IT Governance 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 IT Governance
- The source machine's zone is categorized as IT Governance
- The destination machine is an asset categorized as IT Governance
- The destination machine is an asset under the IT Governance group
- The destination machine's zone is categorized as IT Governance
- The device machine is an asset categorized as IT Governance
- The device machine is an asset under the IT Governance group
- The device machine's zone is categorized as IT Governance

By default, the CIP for IT Governance processes all incoming events.

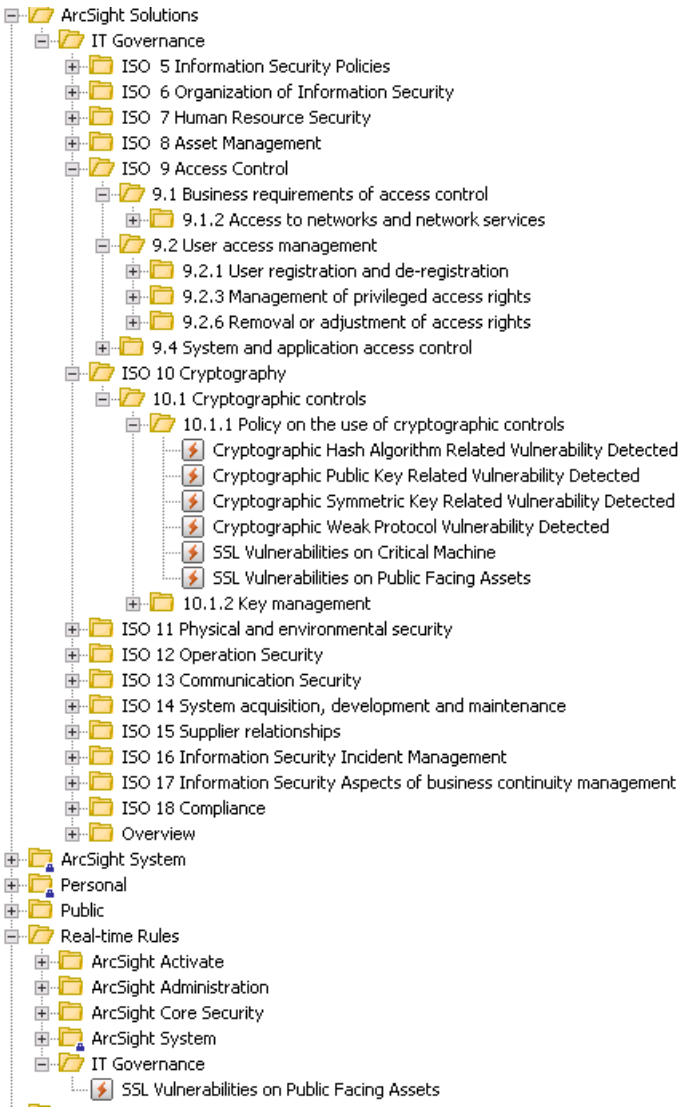
Deploy the Solution for ITGov CIP Rules

In order for a CIP for IT Governance rule to process ITGov-related events, the rule must be deployed to the `Real-time Rules` group. By default, CIP for ITGov 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 to the Real-time Rules group:

1. From the Resources tab in the Navigator panel, go to **Rules** and navigate to the ArcSight Solutions/IT Governance group.
2. Expand the IT Governance folder that contains the rule to deploy and select the Rule. For example, to select "SSL Vulnerabilities on Public Facing Assets" rule,expand /ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls.
3. Drag and drop the Rule from the appropriate /ArcSight Solutions/IT Governance group into the Real-time Rules/IT Governance group.
4. From the Drag & Drop Options dialog, select the **Link** option.

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



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

By default, the CIP for IT Governance rules are disabled. The rules do not trigger until they are deployed and enabled. After you have deployed the CIP for IT Governance 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/IT Governance` 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 IT Governance 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 Deploying Real-time Rules section in the ArcSight ESM Console Online Help.

Enable Data Monitors

All of the CIP's data monitors for IT Governance 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/IT Governance` 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 Compliance Insight Package for ITGov v5.0 are not enabled. Some reports, query viewers, and dashboards require enabled trends to show data.

Shown below is the list of end user resources which requires enabling trends to show data:

Resource	Type	URI	Required Trend
Traffic by Hosts without Asset Mapping	Query Viewer	/All Query Viewers/ArcSight Solutions /IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets	Traffic by Hosts without Asset Mapping
Top User with Machine Access	Report	/All Reports/ ArcSight Solutions /IT Governance/ ISO 9 Access control/ 9.1 Business requirements of access control/ 9.1.1 Access control policy	Daily Machine Access per User
Monitored Account Activity in the Last Day - Template	Report	/All Reports/ ArcSight Solutions /IT Governance/ ISO 9 Access control/ 9.1 Business requirements of access control/ 9.1.1 Access control policy	Monitored Users

Resource	Type	URI	Required Trend
Monitored Account Activity in the Past Week - Template	Report	/All Reports/ ArcSight Solutions /IT Governance/ ISO 9 Access control/ 9.1 Business requirements of access control/ 9.1.1 Access control policy	Monitored Users
Weekly Trend - Configuration Modification Summary	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management	Configuration Changes
Anti-Virus Stopped or Paused in the Last Month	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging	Daily Trend of Anti-Virus Stopped or Paused Events
Number of Successful User Logins over the Past Week	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging	User Login Count
Number of Unsuccessful User Logins over the Past Month	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging	User Login Count
Number of Unsuccessful User Logins over the Past Week	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging	User Login Count
DoS Attacks Weekly Trend	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging	DoS Attacks Trend
Attacks and Suspicious Activity Weekly Trend	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events	Attacks and Suspicious Activities Trend
Average Time to Resolution - By Case Severity	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents	Case History
Average Time to Resolution - By Day	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents	Case History
Average Time to Resolution - By User	Report	/All Reports/ ArcSight Solutions /IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents	Case History
Weekly Trend - Shutdown of Critical Machines	Report	All Reports/ ArcSight Solutions /IT Governance/ ISO 17 Information security aspects of business continuity management/ 17.1.3 Verify, review and evaluate information security continuity	Shutdown of Critical Machines

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, the 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 "The Partition Retention Period (in days), Scheduler Start Time, For general information about trends, see the ArcSight Console User's Guide.

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. ITGovernance includes the ArcSight Solutions/IT Governance group, which holds the cases generated by some IT Governance rules.

You can add more groups to the ArcSight Solutions/IT Governance group or your own group if you want to add more differentiations. If you do add more groups to the ArcSight Solutions/IT Governance 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 ITGovernance directory.

Rule	Case URI
Wireless Malicious Traffic Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Successful Non Secure Remote Access	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Suspicious Activities by New Hires	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Former Employee Account Activity	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Former Employee User Account Access Attempt	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Suspicious Activities by Former Employee	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Removable Media Detected on Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Removable Media Activity
Disallowed Ports Access	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity

Rule	Case URI
Inactive User Account Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Login Activity by a Stale Account	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Suspicious Activities by a Stale Account	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
User Logged in from different IP Addresses	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
User Logged in from Two Countries	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Privileged Account Changes	/All Cases/All Cases/ArcSight Solutions/IT Governance/Account Activity
Successful Attack - Brute Force Login	/All Cases/All Cases/ArcSight Solutions/IT Governance/Login Activity
Password not Changed for Longer than Policy Standard	/All Cases/All Cases/ArcSight Solutions/IT Governance/Password Management
Unsecured Password Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Password Management
Attempted File Changes in Development Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/File Activity
Cryptographic Hash Algorithm Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities
Cryptographic Public Key Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities
Cryptographic Symmetric Key Related Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities
Cryptographic Weak Protocol Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities
SSL Vulnerabilities on Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/SSL Vulnerabilities
SSL Vulnerabilities on Public Facing Assets	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/SSL Vulnerabilities
Invalid or Expired Certificate	/All Cases/All Cases/ArcSight Solutions/IT Governance/PKI
One or more rows have been deleted from the certificate database	/All Cases/All Cases/ArcSight Solutions/IT Governance/PKI
After Hours Building Access by Contractors	/All Cases/All Cases/ArcSight Solutions/IT Governance/Physical Security

Rule	Case URI
Failed Building Access	/All Cases/All Cases/ArcSight Solutions/IT Governance/Physical Security
Local Logon from Badged Out Employee	/All Cases/All Cases/ArcSight Solutions/IT Governance/Physical Security
Critical Network Device Configuration Change Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes
Critical Operating System Change Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes/OS Changes
Malware or Spyware Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Suspicious Internal Trojan Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Worm Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Audit Log Cleared	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes/Audit Log Cleared
Consecutive Unsuccessful Logins to Administrative Account	/All Cases/All Cases/ArcSight Solutions/IT Governance/Login Activity
Unsuccessful Logins to Multiple Administrative Accounts	/All Cases/All Cases/ArcSight Solutions/IT Governance/Login Activity
Security Patch Missing	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/Missing Security Patch
Critical Vulnerability Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/Critical Vulnerabilities
Overflow Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/Overflow Vulnerabilities
SQL Injection Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/SQL Injection Vulnerabilities
Vulnerabilities on Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/Critical Vulnerable Assets
XSRF Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/XSRF Vulnerabilities
XSS Vulnerabilities	/All Cases/All Cases/ArcSight Solutions/IT Governance/Vulnerabilities/XSS Vulnerabilities
Communication between Production and Development Domains	/All Cases/All Cases/ArcSight Solutions/IT Governance/Communication Activity

Rule	Case URI
Communication between Sensitive Asset and Test Domain	/All Cases/All Cases/ArcSight Solutions/IT Governance/Communication Activity
Communication between Sensitive Asset and Third Party Domain	/All Cases/All Cases/ArcSight Solutions/IT Governance/Communication Activity
Possible Covert Channel	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Possible Information Interception	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Possible Redirection Attack	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Possible Traffic Anomaly	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
DoS Detected	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Possible Email Attack	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Potential Distributed DoS	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Information Leak on HR assets	/All Cases/All Cases/ArcSight Solutions/IT Governance/Information Disclosure
Information Leak on of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Information Disclosure
Attack from Third-Party System	/All Cases/All Cases/ArcSight Solutions/IT Governance/Third-Party Incidents
Severely Attacked System	/All Cases/All Cases/ArcSight Solutions/IT Governance/Malicious Activity
Information System Failures of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes/OS Changes
Resource Exhaustion of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes/OS Changes
Shutdown of Highly Critical Machine	/All Cases/All Cases/ArcSight Solutions/IT Governance/Configuration Changes/OS Changes
Organizational Data Information Leak	/All Cases/All Cases/ArcSight Solutions/IT Governance/Information Disclosure
/All Cases/All Cases/ArcSight Solutions/IT Governance/Information Disclosure	/All Cases/All Cases/ArcSight Solutions/IT Governance/Information Disclosure

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 are important to your organization and therefore should be tracked with cases.

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

From the Resources tab in the Navigator panel, go to Rules and navigate to the ArcSightSolutions/IT Governance group.

1. Right-click a rule and select **Edit Rule.**
2. The rule displays in the Inspect/Edit panel.
3. Select the **Action** tab form the Inspect/Edit panel.
4. Right-click the **Add to Existing Case** action and select **Enable Action.**

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 rule in the ArcSight Solutions/IT Governance that triggers on that specific behavior and add actions to those rules to create cases. For example, if you want to create a case every time an account is locked out, edit the Account Lockout 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 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:

- Successful Default Vendor Account Used
- Account Lockout
- Security Software Stopped or Paused
- Suspicious Internal Trojan Detected
- Multiple Cases Created on Short Period

You can enable the notification actions for these rules. You can add a rule action to other `ArcSight Solutions/ITGov` 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 online Help*. This configuration is optional.

Configure Additional Resources

Additional configuration may be required or desired for the individual resources provided to address a specific IT Governance CIP Standard. For more information on resources (including information on asset categorization), see "Resource Reference" on page 41.

Build FlexConnector(s) for Physical Access Devices

The Compliance Insight Package for ITGov v5.0 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 Solution for ITGov CIP 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:

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 type	Object	Behavior	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

Event type	Object	Behavior	Device Group	Outcome	Significance
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.

Chapter 3: Resource Reference

This section includes lists of the following resources:

ISO 5: Information Security Policies Resources

Resource	Type	URI	Description
Policy Violations	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Selects policy violations in the past.
Policy Violations	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Displays information about policy violations and violators.
Top 10 Policy Violations	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 10 policy breach events.

Resource	Type	URI	Description
Top 10 Policy Violators	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 10 policy violators.
Machines Conducting Policy Breaches	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows machines which were involved in policy breaches.
Machines Conducting Policy Violations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows machines which were involved in policy violations.
Policy Violations - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Provides a listing of events categorized by ArcSight as policy violations, which target the various Network Domains by Asset. may (and should) be focused based on the Network Domain of interest.
Policy Violations from Third-Party Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
Top 20 Policy Breach Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 20 policy breach events.
Top 20 Policy Violation Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 20 policy violation events.
Machines Conducting Policy Breaches	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows machines which were involved in policy breaches.

Resource	Type	URI	Description
Machines Conducting Policy Violations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows machines which were involved in policy violations.
Policy Violations - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. may (and should) be focused based on the Network Domain of interest.
Policy Violations from Third-Party Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
Top 20 Policy Breaches Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 20 policy breaches events.
Top 20 Policy Violation Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 5 Information Security Policies/5.1 Management direction for information security/5.1.2 Review of the policies for information security/	Shows the top 20 policy violation events.

ISO 6: Organization of Information Security Resources

Resource	Type	URI	Description
Traffic to and from Classified Machines	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	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 Classified Machines	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Displays information about traffic between assets whose criticality is categorized differently.
Potentially Problematic Remote Access	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Displays information about remote access by privileged users or to insecure systems.
Classification Level Traffic High to Low	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows a graph of network traffic which went from a higher-classified asset to a lower-classified one.

Resource	Type	URI	Description
Classification Level Traffic Low to High	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows a graph of network traffic which went from a lower-classified asset to a higher-classified one.
Last 20 Successful Non Secure Access Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Shows the last 20 successful non secure remote access events.
Non Secure Remote Access Attempts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Shows a moving average of unsuccessful non secure 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	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Displays an Event Graph anytime a connection is reported by a VPN device, where the user name belongs to a privileged account.
Attacks from Development Targeting Production	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Provides a listing of hostile or suspicious traffic from development machines targeting production facilities.

Resource	Type	URI	Description
Attacks from Production Targeting Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.
Low to High Classified Asset Communication	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.
Multiple Functions Implemented on a Server	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Returns all assets that implement multiple functionalities; for example, a database and Web server installed on the same machine.

Resource	Type	URI	Description
Operations and Development Cross-Talk	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Returns all assets that are shared between at least two of the Test, Development and Operation domains.
Wireless Encryption Violations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.1 Mobile device policy/	Returns all wireless encryption violations detected by a wireless Intrusion Detection System (IDS) in the last 24 hours.
All VPN Access Attempts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Provides an overview of the number of VPN access attempts by non-administrative users.

Resource	Type	URI	Description
Privileged VPN Remote Access Attempts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Shows all connections reported by a VPN device, where the user name belongs to a privileged account.
Unsuccessful VPN Access	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Lists all failed VPN access attempts.
Attacks from Development Targeting Production	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all cross-talk in the last 24 hours between assets in Development category and assets in Test category.

Resource	Type	URI	Description
High to Low Classified Asset Communication	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.
Low to High Classified Asset Communication	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.
Multiple Functions Implemented on a Server	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation 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/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Returns all assets that are shared between at least two of the Test, Development, and Operation domains.

Resource	Type	URI	Description
Test and Operations Cross-Talk	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.1 Internal organization/6.1.2 Segregation of duties/	Shows all cross-talk in the last 24 hours between assets in Test category and assets in Operations category.
Count of Attacks and Suspicious Activity Event Names in the Wireless Network Domain	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.1 Mobile device policy/	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/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.1 Mobile device policy/	Shows all wireless encryption violations.

Resource	Type	URI	Description
All VPN Access Attempts	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Lists all VPN access attempts.
Privileged VPN Remote Access Attempts	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	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.
Unsuccessful VPN Access	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 6 Organization of Information Security/6.2 Mobile devices and teleworking/6.2.2 Teleworking/	Provides a listing of failed VPN access, the number of such failed events and the last failure time.

ISO 7: Human Resource Security Resources

Resource	Type	URI	Description
New Hires Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows information related to activity by new hire employees.
Former Employee Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Shows information related to activity by former employees.
Internet Activity by New Hires	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows Internet activity per reporting device per new hire over a day's period.
New Hires Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows the new hire user logins.

Resource	Type	URI	Description
Suspicious Activity by New Hires	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	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).
After Hours Successful New Hire Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows details of all after hours successful new hire logins within the last day.
All Events by New Hires	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows all events by new hires.
All Suspicious Events by New Hires	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows all suspicious events by new hires based on the event table.
New Hire Account Added to Groups	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows all new hire accounts added to groups.
New Hire Internet Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	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.
Summary of Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays the number of suspicious events per new hire.
Suspicious Activity by New Hires	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all the identified suspicious activity performed by new users.
Unsuccessful New Hire Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows details of all unsuccessful user logins within the last day.
Activity by Former Employees	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Shows any activity performed by users who are known to be terminated.

Resource	Type	URI	Description
Former Employee Account Access Attempt	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Lists all log-in activity from a former employee.
Former Employee Accounts in Use	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Identifies all former employee user names and reporting device details associated with recent events.
Suspicious Activities by Former Employee	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Lists all suspicious Activities by former employee.
All Events by New Hires	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows all events by new hires.
Suspicious Activities by New Hires	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows ???
Former Employee Accounts in Use	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Identifies all former employee user names and reporting device details associated with recent events.
After Hours Successful New Hire Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all after hours successful new hire logins within the last day.
New Hire Account Added to Groups	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all after hours unsuccessful new hire logins within the last day.
New Hire Internet Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all the identified suspicious activity performed by new users.
Summary of Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Shows a summary of attacks and suspicious events by new hires.

Resource	Type	URI	Description
Suspicious Activity by New Hires	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all the identified suspicious activity performed by new users.
Unsuccessful New Hire Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.1 Prior to employment/7.1.1 Screening/	Displays all after hours unsuccessful new hire logins within the last day.
Activity by Former Employees	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Shows any activity performed by users who are known to be terminated.
Former Employee Account Access Attempt	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Lists all login activity from any former employee.
Suspicious Activities by Former Employee	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 7 Human resource security/7.3 Termination and change of employment/7.3.1 Termination or change of employment responsibilities/	Lists all suspicious activities by any former employee.

ISO 8: Asset Management Resources

Resource	Type	URI	Description
Last State External Device Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.3 Media handling/8.3.1 Management of removable media/	Provides real-time display of the last 20 external device activities and their status.
Last State External Device Overview	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.3 Media handling/8.3.1 Management of removable media/	Shows a real-time display of the last 20 external device activity and their status.
Assets in Partners Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Partners Network Domain.

Resource	Type	URI	Description
Assets in the Development Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Development Network Domain.
Assets in the Operations Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Operation Network Domain.
Assets in the Production Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Production Network Domain.
Assets in the Public-Facing Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Public-Facing Network Domain.
Assets in the Test Network Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Test Network Domain.
Assets in the Third Party Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Third Party Domain.
DNS Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all of assets which are categorized as DNS systems.
Database Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all of assets which are categorized as databases.
Email Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Email Network Domain.
Financial assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Financial Network Domain.

Resource	Type	URI	Description
Human Resources Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Human Resources Domain.
Web Application Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all of assets which are categorized as web applications.
Wireless Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of all the assets for the Wireless Network Domain.
Asset Creation by Location	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of newly created assets.
Asset Deletion by Location	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of deleted assets.
Asset Identification Report	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Shows all assets and their respective network domain.
Asset Modification by Location	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of modified assets.
Assets by Application Type - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a list of all the assets for the environments. 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/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a list of all the assets for the various network domains. May (and should) be focused based on the network domain of interest. Results are sorted by creation time.
Hosts without Asset Mapping	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Shows all traffic from or to hosts that are not mapped to any asset on ESM.

Resource	Type	URI	Description
Non-Operating System Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets which are categorized as non-OS Systems.
Operating System Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets which are categorized as OS Systems.
Traffic by Hosts without Asset Record - Trend Base	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Returns all traffic by hosts that are not mapped to an asset on ESM.
Assets by Owner	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.2 Ownership of assets/	Provides the listing of all the assets listed by owners.
Assets without Assigned Owner	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.2 Ownership of assets/	Provides the listing of all the assets without owners.
Classification of Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	Shows the asset classifications sorted by network domain.
Critical Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	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/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	Shows the asset criticality sorted by their criticality and network domain.
Removable Media Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.3 Media handling/8.3.1 Management of removable media/	Shows all the removable media activity for the last 24 hours.

Resource	Type	URI	Description
Traffic by Hosts without Asset Mapping	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Shows all traffic to or from hosts not mapped to any asset on ESM. Note: the traffic shown is not current, and is based on the underlying trend.
Asset Creation by Location	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of newly created assets.
Asset Deletion by Location	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of deleted assets.
Asset Identification Report	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Shows all assets and their respective network domain.
Asset Modification by Location	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides a listing of modified assets.
Assets by Application Type - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets by application type. 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/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets for the various Network Domains. May (and should) be focused based on the network domain of interest. Results are sorted by creation time.
Non-Operating System Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets which are categorized as non-OS Systems. 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/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Provides the listing of all the assets which are categorized as OS Systems. May (and should) be focused based on the application type of interest. Results are sorted by creation time.
Assets by Owners	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.2 Ownership of assets/	Provides a listing of newly created assets.

Resource	Type	URI	Description
Assets without Assigned Owner	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.2 Ownership of assets/	Provides a listing of newly created assets.
Classification of Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	Shows the asset classifications sorted by network domain.
Critical Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	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/IT Governance/ISO 8 Asset management/8.2 Information classification/8.2.1 Classification of information/	Shows the asset criticality sorted by their criticality and network domain.
Removable Media Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.3 Media handling/8.3.1 Management of removable media/	Shows all the removable media activity for the last 24 hours using Windows events.
Traffic by Hosts without Asset Mapping	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 8 Asset management/8.1 Responsibility for assets/8.1.1 Inventory of assets/	Stores all traffic related to a host that is not mapped to any asset on ESM. Note that this trend only reflects the asset information at the time the trend runs.

ISO 9: Access Control Resources

Resource	Type	Uri	Description
Default Vendor Account Used	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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.
Privileged Account Changed	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.3 Management of privileged access rights/	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.
Account Authorization Changes Summary	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Shows a real-time feed of events reflecting account access rights is attempted to be changed.
Removal of Access Rights	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	Shows a live feed of events reflecting the removal of a user's access privileges.

Resource	Type	Uri	Description
Account Lockouts	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Shows events where a rule fired to lock out a user ID.
User Activities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Displays information about uses of default vendor and other suspicious accounts.
Disallowed Ports Communications	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Displays information around events to disallowed ports.
Account Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Shows information related to user account activity.
Default Vendor Account Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Shows the users of default vendor accounts.
Privileged Account Changes	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays information where changes have been made to an administrative account.

Resource	Type	Uri	Description
User Group Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Shows information related to user group activity.
Account Lockouts	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Displays information about account lockouts.
Failed User Actions	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all failed user actions in the last hour.
Last 50 User Activities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the last 50 user activities.
Successful User Actions	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the moving average number of successful user actions in the last hour.

Resource	Type	Uri	Description
Top 10 Users with Failed Actions	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the top 10 non-administrative attacker and target user pairs with failed actions in the last hour.
Disallowed Ports by Policy	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Provides the distribution of disallowed ports by policies.
Last Connections to Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows the last 10 connections to disallowed ports to or from the network.
Top Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Provides a list of the top 10 disallowed ports.
Top Internal Hosts to Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Provides a list of the top 10 internal hosts that accessed disallowed ports.

Resource	Type	Uri	Description
Top Internal Providers of Disallowed Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Provides a list of the top 10 internal providers of disallowed ports.
Last 10 Privileged Account Changes	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays events where authorization/access changes have been made to an administrative account.
Last 20 Information System Accounts Created	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 account creations.
Last 20 Information System Accounts Deleted	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 account deletions.
Last 20 Information System Accounts Modified	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 account modifications.
Last 20 User Group Created	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 user group creations.
Last 20 User Group Deleted	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 user group deletions.

Resource	Type	Uri	Description
Last 20 User Group Modified	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the last 20 user group modifications.
Last Default Vendor Account Credentials Observed	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays login events where user has attempted to login to a system with vendor-supplied default User ID.
Top 10 Asset Network Domains with Account Creation Deletion and Modification	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays the Network Domains asset categories in which the most accounts have been created, modified or deleted.
Top 10 Privileged Account Changes	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays top changed administrative accounts.
Top Default Vendor Accounts Observed	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays top vendor-supplied default account observed.
Top TarRetrieves with Default Vendor Accounts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Displays login events where user has attempted to login to a system with vendor-supplied default account.
Users Changing Accounts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/	Shows the users that added, deleted and modified accounts.

Resource	Type	Uri	Description
Account Lockouts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Displays events when an account has been locked out; triggered by a related rule firing.
Failed User Actions	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Identifies failed non-administrative actions.
Monitored User	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Identifies events with monitored users. These events are defined as such in which either the source or destination users are monitored users. Monitored users are stored in the Active List "Monitored Accounts".
Successful User Actions	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Identifies successful non-administrative actions.
Disallowed Ports Access	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Tracks all connections to disallowed ports.

Resource	Type	Uri	Description
Disallowed Ports Access from Internal Hosts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Tracks all connections to disallowed ports from internal hosts.
Disallowed Ports Access to Internal Hosts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Tracks all connections to disallowed ports hosted by internal hosts.
Insecure Services	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Selects events based on inherently insecure services.
Account Creation	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies account creation events.
Account Deletion	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies account deletion events.

Resource	Type	Uri	Description
Default Vendor Account Access Attempted	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies events where system access with vendor-supplied accounts is attempted.
Default Vendor Account Credential Observed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies events where system access with vendor-supplied accounts is observed.
Direct Root or Administrator Credential Observed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies events where system access with root or administrator credential is observed.
Login Activity by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies login activities by accounts that are on the Stale Accounts active list.
Suspicious Activities by Stale User Accounts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies suspicious activities by accounts that are on the Stale Accounts active list.

Resource	Type	Uri	Description
User Group Creation	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies user group creation events.
User Group Deletion	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies user group deletion events.
Privileged Account Changes	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.3 Management of privileged access rights/	Selects events where a change is attempted to a privileged account (as defined by the referenced active list).
Access Rights Changes	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Selects events where a change was attempted for account access rights.
Account Creations, Modifications and Deletions	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Identifies all account management events.

Resource	Type	Uri	Description
Account Modification	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Identifies account modification events.
User Added to Group	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Identifies when a user is added to a group.
User Group Modification	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Identifies user group modification events.
User Removed from Group	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Identifies when a user removed from group.
Removal of Access Rights	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	Identifies events indicating a user access right is removed. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.

Resource	Type	Uri	Description
Account Lockouts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.
All Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies all types of Brute Force Login Attempts.
Application Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies all application brute force login attempt events.
IDS Detected Brute Force Login Attempts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Shows events sent by Intrusion Detection Systems that indicate brute force login attempts.
IDS Detected Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Selects events from Intrusion Detection Systems that indicate a successful brute force login has occurred.

Resource	Type	Uri	Description
Successful Brute Force Logins	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies events generated by the Probable Successful Brute Force rule that involve assets categorized in one of your Network Domains.
Failed Password Change	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Identifies unsuccessful password change events.
Password Change Attempts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	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.
Successful Password Change	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Identifies successful password change events.
Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Detects configuration modifications.

Resource	Type	Uri	Description
File Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Identifies all file changes.
Successful Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Identifies successful configuration modifications.
Traffic from Others to Development	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Selects all traffic destined for the development segment (s) of the network that did not originate from within a development segment.
Unsuccessful Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Identifies unsuccessful configuration modifications.
Account Creations in Development	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Shows all account creations on development systems.

Resource	Type	Uri	Description
Account Deletions in Development	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Provides a listing of Information System accounts that were deleted in a development domain.
Account Modifications in Development	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Shows all account modifications in development domain.
Attempted File Changes in Development Originated from Operations	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays attempts to change a file on a host in the development segment from a source that is in operations.
Attempted File Changes in Development Originated from Partners	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays attempts to change a file on a host in the development segment from a source that is in partner.
Attempted File Changes in Development Originated from Production	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays attempts to change a file on a host in the development segment from a source that is in production.

Resource	Type	Uri	Description
Attempted File Changes in Development Originated from Public-Facing	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays attempts to change a file on a host in the development segment from a source that is in Public-Facing.
Attempted File Changes in Development Originated from Test	FocusedReport	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays attempts to change a file on a host in the development segment from a source that is in Third Party.
Daily User Machine Access	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows a summary of machine accesses by a user per day.
Detail Monitored Account Activities in the Last Day - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of a user being monitored within the last day. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Individual Account Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activity of a particular user. The user name is a required parameter for this report.

Resource	Type	Uri	Description
Monitored Account Activities in the Last Day by Hour - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of a user being monitored within the last day by hour. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Monitored Account Activities in the Past Week - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of one of the users being monitored within the past week. The user name is stored in the Active List "Monitored Accounts" and has to be provided when using this query.
Monitored Account Asset Access in the Last Day by Hour - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the number of assets accessed by one of the users being monitored within the past week. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Monitored Account Asset Access in the Past Week - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the number of assets accessed by one of the users being monitored within the past week. The user name is stored in the Active List "Monitored Accounts" and has to be specified when using this query.
Monitored Users	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	identifies monitored users. Monitored accounts are stored in the Active List "Monitored Accounts".
Top 100 Most Active Users	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Lists the top 100 most active users over the past day.

Resource	Type	Uri	Description
Top User with Machine Access in the Last Day	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the top users with most machine accesses in a day.
Top User with Machine Access in the Past Month	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the top users with most machine accesses in the past month.
User Activity Summary	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows a summary of user activity.
Disallowed Ports	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows traffic that should not be seen per the Allowed Ports active list.
Disallowed Ports by Connection Types	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows the top disallowed ports grouped by connection types.
Inbound Insecure Transmissions	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.

Resource	Type	Uri	Description
Insecure Transmissions	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Internal Insecure Service Providers	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Returns the internal providers of insecure services.
Top Disallowed Ports	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows the top disallowed ports.
Top Internal Hosts Accessed Disallowed Ports	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows the top internal hosts that accessed most disallowed ports.
Top Internal Hosts Provided Disallowed Ports	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows the top internal hosts that provided most disallowed ports.

Resource	Type	Uri	Description
Unencrypted Services by Host Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Returns all unencrypted services by a particular host name identified in the last 24 hours using vulnerability and port scanning events.
Account Creations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Provides a listing of all Information System accounts that were created.
Account Creations in Network Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Provides a listing of all Information System accounts that were deleted.
Account Deletions in Network Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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.

Resource	Type	Uri	Description
Detail Default Vendor Account Used	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows if a vendor supplied user account without password is being used to login.
Inactive User Accounts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all user names that are in the Stale Accounts active list.
Login Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows stale user accounts from which login activity was attempted.
Suspicious Activity by Stale User Accounts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows suspicious activities of stale user accounts.
Systems Accessed by Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all systems that users have tried to access directly as root or administrator.

Resource	Type	Uri	Description
Top Attackers Attempted Default Vendor Accounts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top hosts from which attackers most attempted default vendor account.
Top Attackers Using Default Vendor Account	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top attackers who successfully used a vendor supplied user account.
Top Attackers Using Direct Root or Administrator Account	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top attackers attempting use of direct root or administrator credential.
Top Default Vendor Accounts Attempted	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top vendor supplied user account still being used to login.
Top Default Vendor Accounts Used	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top vendor supplied user account still being used to login.

Resource	Type	Uri	Description
Top Target Hosts Where Default Vendor Account Attempted	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows the top hosts where direct root or administrator account is attempted.
User Group Creations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Provides a listing of all Information User Groups that were created.
User Group Deletions	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Provides a listing of all Information User Groups that were deleted.

Resource	Type	Uri	Description
User Logged in from Two Countries	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Selects user names that have been used to login from two different countries.
User Logged in from different IP Addresses	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Selects single user names that have been used to login from different IP addresses.
Privileged Account Change Details	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.3 Management of privileged access rights/	Lists details of events regarding changes to privileged accounts.
Account Authorization Changes Summary	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Lists details of events regarding changes to account authorization.
Account Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Provides a listing of all Information System accounts that were modified.

Resource	Type	Uri	Description
Account Modifications in Network Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Provides a listing of Information System accounts that were modified 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.
Users Added to Groups	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Provides a listing of all Information of Users which added to Groups.
Users Removed from Groups	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Provides a listing of all Information of Users which removed from Groups.
Failed or Attempted Removal of Access Rights	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	Shows all failed or attempted removal of access rights from a host resource.
Successful Removal of Access Rights	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	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.

Resource	Type	Uri	Description
Account Lockouts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Retrieves all information about account lockouts.
Account Lockouts per System	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Counts account lockouts per user and system.
Application Brute Force Login Attempts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies all user names for which there are a continuous set of unsuccessful login attempts.

Resource	Type	Uri	Description
Frequent Unsuccessful Logins from Attacker Host	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies all target hosts which have received a continuous set of unsuccessful login attempts.
Successful Brute Force Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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.
All Password Change Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Provides a list of all password change events and their outcome.
Failed Password Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Retrieves failed password change events, ordered by target user name.

Resource	Type	Uri	Description
Passwords not Changed for Longer than Policy Standard	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Lists accounts for which the password was not changed for longer than the policy standard permits.
Successful Password Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Lists successful password change events, ordered by target user name.
Unsecured Password Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Retrieves unsecured password events.
Attempted File Changes in Development originated from Other Network Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Counts the number of creations, deletions and modifications of files on systems in the development network domain.

Resource	Type	Uri	Description
Successful Administrative Logins to Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Identifies successful logins with an administrative account to development systems.
Successful Configuration Changes to Development Machines	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Lists a count of successful configuration changes made to development systems.
Successful User Logins to Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Retrieves all successful user logins to development.
Suspicious Activity in Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Shows suspicious activities in the Development Network Domain.
Unsuccessful Administrative Logins to Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Retrieves failed logins using an administrative account, to assets categorized as Development.

Resource	Type	Uri	Description
Unsuccessful User Logins to Development	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Retrieves failed logins with a non-administrator account to assets categorized as Development.
Monitored Account Activity in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of monitored users in the last 2 hours.
Top 100 Most Active Users	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Lists the top 100 most active users over the past day.
User Activity Summary	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows a summary of user activity.
Account Lockouts	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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.

Resource	Type	Uri	Description
Password Changes	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Shows all password change events.
Individual Account Activity in the Last Day	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of a particular user within 1 day. The user name is a required parameter for this report.
Monitored Account Activity in the Last Day - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of a monitored user in the last day. The user name is stored in the Active List "Monitored Accounts" and has to be specified when running this report.
Monitored Account Activity in the Past Week - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows all activities of a monitored user in the past week. The user name is stored in the Active List "Monitored Accounts" and has to be specified when the report is run.
Top User with Machine Access	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Shows the top users with most distinct machines accessed in the last month.
Detail Disallowed Port Access	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows traffic that should not be seen per the Allowed Ports/Disallowed Ports active list.

Resource	Type	Uri	Description
Disallowed Port Access Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Shows several summary aspects of traffic to disallowed ports.
Inbound Insecure Transmissions	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Lists all inbound traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Insecure Transmissions	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Lists all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
Internal Insecure Service Providers	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Lists all internal providers of insecure services.
Unencrypted Services by Host Name	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	returns all unencrypted services by a particular host name (by default localhost) identified in the last 24 hours using vulnerability and port scanning events.

Resource	Type	Uri	Description
Account Creations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all account creations.
Account Creations in Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	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. 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/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all account deletions.
Account Deletions in Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Provides a listing of Information System accounts that were deleted in a specific network domain. 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.
Attempted Default Vendor Accounts - Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows summary views of events and systems when a vendor supplied user account is attempted by a user to login.

Resource	Type	Uri	Description
Attempted Direct Root or Administrator	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows events and systems when direct root or administrator account is attempted by a user to login.
Detail Specific Default Vendor Account Uses	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all logins using a specific vendor supplied user account.
Inactive User Account Detected	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all user names that are in the Stale Accounts active list.
Login Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows login activity by users that are on the Stale Accounts Active List. The report is ordered by the outcome of the login event.
Successful Default Vendor Account Used - Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows high level summary views of events when a vendor-supplied user account is used to login.

Resource	Type	Uri	Description
Suspicious Activity by Inactive Users	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows suspicious activity by users that are on the Stale Accounts Active List.
Systems Accessed by Default Vendor Accounts	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all systems that users have tried to access as a default vendor account.
User Group Account Creations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all user group creations.
User Group Account Deletions	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows all user group deletions.
User Logged in from Different IP Addresses	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows user names that have been used to login from different IP addresses in very short period. This may indicate user name sharing.

Resource	Type	Uri	Description
User Logged in from Two Countries	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.1 User registration and de-registration/	Shows user names that have been used to login from two different countries. This may indicate user name sharing.
Privileged Account Change Details	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.3 Management of privileged access rights/	Lists details of events when an Privileged account was attempted to be changed.
Account Authorization Changes Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Shows a summary of account authorization changes.
Account Modifications	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Shows all account modifications.
Account Modifications in Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Provides a listing of Information System accounts that were modified in a specific network domain. 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.

Resource	Type	Uri	Description
Users Added to Groups	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Shows all user accounts added to groups.
Users Removed from Groups	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.5 Review of user access rights/	Shows all users accounts removed from groups.
Failed or Attempted Removal of Access Rights	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	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.
Successful Removal of Access Rights	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	Shows 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.
Account Lockouts per System	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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.

Resource	Type	Uri	Description
Account Lockouts per User and System	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Shows application brute force login attempts.
Frequent Unsuccessful Logins by User Name	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Lists all target hosts which have received a continuous set of unsuccessful login attempts.

Resource	Type	Uri	Description
Successful Brute Force Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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.
All Password Change Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Provides a list of all password change events, ordered by the time in which they occurred.
Failed Password Changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Displays failed password change events.
Passwords not Changed for Longer than Policy Standard	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Lists passwords that were not changed for longer than the policy standard.
Successful Password Changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Displays successful password change events.

Resource	Type	Uri	Description
Unsecured Password Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.3 Password management system/	Displays unsecured password events.
Attempted File Changes in Development Originated from Other Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	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/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	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	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays all successful administrative logins to assets categorized as Development.
Successful Configuration Changes to Development Machines	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Shows a count of successful configuration changes made to development systems.

Resource	Type	Uri	Description
Successful User Logins to Development	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays all successful non-administrative logins to assets categorized as Development.
Suspicious Activity in Development	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Shows suspicious activity by users on the development domain.
Unsuccessful Administrative Logins to Development	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays all failed logins with an administrative account to assets categorized as Development.
Unsuccessful User Logins to Development	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 9 Access control/9.4 System and application access control/9.4.5 Access control to program source code/	Displays all failed logins with non-administrative account to assets categorized as Development.
Removal of Access Rights	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.6 Removal or adjustment of access rights/	Triggers when events indicating the following are detected: 1). Either a user is removed from a host, or 2). User's authentication privileges are modified.

Resource	Type	Uri	Description
Account Lockout	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Detects account lockouts. This activity is suspicious.
Brute Force Login Attempts	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Identifies brute force login attempts.
Frequent Unsuccessful Logins by User Name	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	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/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Fires when it notices a high frequency of unsuccessful logins on the same target host.

Resource	Type	Uri	Description
Successful Attack - Brute Force Login	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.2 Secure log-on procedures/	Detects successful brute force login attacks.
Attempted File Changes in Development Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.5 Access control to program source code/	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.
Disallowed Ports Access	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	Triggers when traffic to a forbidden target port occurs.
Inactive User Account Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	Fires every time an entry ages out of the Stale Accounts active list.
Internal Insecure Service Provider Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.1 Business requirements of access control/9.1.2 Access to networks and network services/	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.

Resource	Type	Uri	Description
Login Activity by a Stale Account	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	Identifies login activities by accounts that are on the Stale Accounts active list.
Password not Changed for Longer than Policy Standard	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.3 Password management system/	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.
Privileged Account Changes	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.3 Management of privileged access rights/	Fires whenever an access/authorization change is attempted to be made to an administrative account. A case is created for each such incident.
Successful Default Vendor Account Used	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	Selects successful access to system using default user accounts.
Successful Password Change	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.3 Password management system/	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.

Resource	Type	Uri	Description
Suspicious Activities by a Stale Account	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	identifies suspicious activities by accounts that are on the Stale Accounts active list.
Unsecured Password Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.4 System and application access control/9.4.3 Password management system/	Detects unsecured passwords.
User Logged in from Two Countries	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	Fires when someone is using the same user name to login from two different countries. This may indicate user name sharing.
User Logged in from different IP Addresses	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 9 Access Control/9.2 User access management/9.2.1 User registration and de-registration/	Fires when someone is using the same user name to login from different ip addresses. This may indicate user name sharing.
Daily Machine Access per User	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Stores the summary of machine accesses per user per day.
Monitored Users	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 9 Access control/9.1 Business requirements of access control/9.1.1 Access control policy/	Stores all events that are related to a monitored user either in the target or attacker fields.

ISO 10: Cryptography Resources

Resource	Type	URI	Description
Invalid or Expired Certificate Presented	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows a real-time feed of events which indicate that an invalid or expired certificate was detected.
Cryptographic Hash Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides an overview of Cryptographic Hash Vulnerabilities.
Cryptographic Public Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides an overview of Cryptographic Public Key Related Vulnerabilities.
Cryptographic Symmetric Key Related Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides an overview of Cryptographic Symmetric Key Related Vulnerabilities.
Cryptographic Weak Protocol Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides an overview of Cryptographic Weak Protocol Vulnerabilities.
SSL Vulnerabilities	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides an overview of SS Vulnerabilities.
Last 10 Cryptographic Hash Algorithm Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the last 10 cryptographic hash related vulnerabilities.
Last 10 Cryptographic Public Key Related Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the last 10 cryptographic public key related vulnerabilities.
Last 10 Cryptographic Symmetric Key Related Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the last 10 cryptographic symmetric key related vulnerabilities.
Last 10 Cryptographic Weak Protocol Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the last 10 cryptographic weak protocol related vulnerabilities.
Last 10 SSL Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the last 10 SSL vulnerabilities.

Resource	Type	URI	Description
Top 10 Cryptographic Hash Algorithm Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the top 20 assets with security patches missing.
Top 10 Cryptographic Public Key Related Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the top 10 assets with cryptographic public key related vulnerabilities.
Top 10 Cryptographic Symmetric Key Related Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the top 10 assets with cryptographic symmetric Key related vulnerabilities.
Top 10 Cryptographic Weak Protocol vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the top 10 assets with cryptographic weak protocol-related vulnerabilities.
Top 10 SSL Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 10 Cryptography/	Provides real-time display of the top 10 assets with SSL vulnerabilities.
Cryptographic Hash Algorithm Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Cryptographic Public Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
Insecure Cryptographic Storage Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that Insecure cryptographic storage has been detected.
SSH Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that an SSH vulnerability was detected.

Resource	Type	URI	Description
SSL Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that an SSL vulnerability was detected.
VPN Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that a VPN vulnerability was detected.
Invalid or Expired Certificate	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Selects events which indicate that an invalid or expired certificate was detected.
Cryptographic Hash Algorithm Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential hash algorithm related vulnerability was detected.
Cryptographic Public Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential symmetric key related vulnerability was detected.
Cryptographic Weak Protocol Vulnerability Detected	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that potential cryptographic weak protocol related vulnerability was detected.
Insecure Cryptographic Storage	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that insecure cryptographic storage has been detected.
SSH Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that SSH vulnerability has been detected.
SSL Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that SSL vulnerability has been detected.

Resource	Type	URI	Description
VPN Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Selects events indicating that VPN vulnerability has been detected.
Certificate Services Backup and Archive Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows Certificate Service Backup Activity based on Windows events.
Certificate Services Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows Certificate Service configuration changes using Windows events.
Certificate Services Started or Stopped	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows when Certificate Service started or stopped using Windows events.
Invalid or Expired Certificate	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows incidents which indicate that an invalid or expired certificate was detected.
Cryptographic Hash Algorithm Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all cryptographic hash algorithm vulnerabilities that have been detected.
Cryptographic Public Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all cryptographic public key vulnerabilities that have been detected.
Cryptographic Symmetric Key Related Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all cryptographic symmetric key vulnerabilities that have been detected.
Cryptographic Weak Protocol Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all cryptographic weak protocol vulnerabilities that have been detected.
Insecure Cryptographic Storage	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all insecure cryptographic assets events identified in the last 24 hours.

Resource	Type	URI	Description
SSH Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all SSL vulnerabilities that have been detected.
SSL Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all SSL vulnerabilities that have been detected.
VPN Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Shows all VPN vulnerabilities that have been detected.
Certificate Services Backup and Archive Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows incidents which indicate that an invalid or expired certificate was detected.
Certificate Services Changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows Certificate Service configuration changes using Windows events.
Certificate Services Started or Stopped	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows when Certificate Service started or stopped using Windows events.
Invalid or Expired Certificate	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Shows incidents which indicate that an invalid or expired certificate was detected.
Cryptographic Hash Algorithm Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when potential cryptographic hash algorithm related vulnerability is detected.
Cryptographic Public Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when potential cryptographic public key related vulnerability was detected.
Cryptographic Symmetric Key Related Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when potential cryptographic symmetric key related vulnerability was detected.

Resource	Type	URI	Description
Cryptographic Weak Protocol Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when potential cryptographic weak protocol related vulnerability was detected.
SSL Vulnerabilities on Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when SSL vulnerability is detected on critical assets.
SSL Vulnerabilities on Public Facing Assets	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.1 Policy on the use of cryptographic controls/	Triggers when SSL vulnerability is detected on public-facing assets.
Invalid or Expired Certificate	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Detects invalid or expired Certificates.
One or more rows have been deleted from the certificate database	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 10 Cryptography/10.1 Cryptographic controls/10.1.2 Key management/	Detects if one or more rows have been deleted from the certificate database using Windows events.

ISO 11: Physical and Environmental Security Resources

Resource	Type	URI	Description
Physical Security	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows all physical access related activities.
Physical Security Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Displays information around physical access.
Building Access - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Used to show the hour of day that users are accessing buildings.

Resource	Type	URI	Description
Contractor Access After Hours	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows the top contractors accesses after hours.
Last 20 Building Access Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows the last 20 physical access events.
Top Users Accessing Buildings	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows the top 10 users accessing buildings.
Badge Out	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Identifies badge out event.
Building Access	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Selects all building access events.
Contractor Access After Hours	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Identifies contractors accessing buildings after hours.
Physical Access Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Selects all events sent to ArcSight ESM by physical security systems.
Successful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Identifies a successful badge-in event.
Successful Building Access Granting	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Identifies granting user access to a building.

Resource	Type	URI	Description
Unsuccessful After Hours Building Access	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Identifies an unsuccessful badge-in event.
Building Access and Leave by User	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access events at all times.
Failed After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows failed attempts to leave a building at any time.
Successful After Hours Building Accesses	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access events at all times.
Successful Building Access Granting	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows all successful building access granting.
Successful Building Leaving Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows all successful building leaving events at all times (for badge reader systems support this option).
Building Access and Leave by User	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access and leave events by user.

Resource	Type	URI	Description
Failed After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows failed attempts to enter a building at any time.
Successful After Hours Building Accesses	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access events.
Successful Building Access Granting	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access-granting events.
Successful Building Leaving Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Shows successful building access events at all times.
Badged Out Employee	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Detects when someone leaves a building and adds the user to the Badged Out active list.
Failed Building Access	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Detects failed physical building access.
Local Logon from Badged Out Employee	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Detects a local logon event though the employee is badged out.

Resource	Type	URI	Description
Successful Badge In	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	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/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Detects when someone leaves a building and removes the user from the badged in active list.
After Hours Building Access by Contractors	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 11 Physical and environmental security/11.1.2 Physical entry controls/	Detects building access events after business hours by contractors.

ISO 12: Operation Security Resources

Resource	Type	URI	Description
Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects non-ArcSight events that indicate configuration changes.
Database Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects database configuration change events.
Firewall Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects firewall configuration change events.
Network IDS Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects NIDS configuration change events.

Resource	Type	URI	Description
Network Routing Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects network routing configuration change events.
Operating System Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects OS configuration change events.
VPN Configuration Changes	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects VPN configuration change events.
Failed Virus Removal Attempt	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects events when an attempt to remove or quarantine a virus on a host failed.
Login Attempts	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows a real-time feed of events where a login attempt was made.
Logouts	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows a real-time feed of logout events.
Audit Log Cleared	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Selects events that indicate an audit log is cleared.
Software Changes in Operations	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Selects events that indicate software changes on operations assets.

Resource	Type	URI	Description
Vulnerability Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events that indicate the existence of vulnerabilities in IT Governance assets.
Information System Audit Tool Logins	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.7 Information systems audit considerations/12.7.1 Information systems audit controls/	Shows all the logins to the Information System Audit Tool - ArcSight.
Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays information about configuration changes.
Firewall Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays information about firewall configuration changes.
Network Devices Configuration Changes Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays information about network devices equipment (such as router, switch, NIDS) configuration changes.
Operating Systems Configuration Modifications Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays information about OS configuration changes.
Malicious Code Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows an overview of the malicious code activity on the organization.

Resource	Type	URI	Description
Anti-Virus Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows an overview of the anti-virus activity on the organization.
General User Login Attempts	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows an overview of user login attempts on the organization.
Unsuccessful User Logins	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows an overview of unsuccessful user activity on the organization.
User Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows an overview of the user login and logouts activity on the organization.
Audit Log Cleared	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Displays Audit Log Cleared compliant status.
Administrative Logins and Logouts	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows an overview of the administrative login and logouts activity on the organization.
Unsuccessful Administrative Logins	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows an overview of unsuccessful administrative logins activity on the organization.
Missing Security Patches	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Displays missing security patches.

Resource	Type	URI	Description
Last State Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	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
Overflow Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of overflow vulnerability events.
SQL Injection Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of SQL injection vulnerability events.
Vulnerability Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of vulnerability events.
XSRF Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of XSRF vulnerability events.
XSS Vulnerabilities Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of XSS vulnerability events.
Peer to Peer Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Displays information related to peer-to-peer activities.

Resource	Type	URI	Description
Last 10 Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent system configuration modifications.
Last 10 Firewall Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent firewall configuration modifications.
Last 10 Network Devices Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent network devices configuration modifications.
Last 10 Network IDSs Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent NIDSs configuration modifications.
Last 10 Network Routing Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent network routing configuration modifications.
Last 10 Operating Systems Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the most recent OS configuration modifications.
Top 10 Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the top 10 system configuration modifications.

Resource	Type	URI	Description
Top 10 Devices with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the assets that have their configurations changed frequently.
Top 10 Firewall Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the top 10 firewall configuration modifications.
Top 10 Firewalls with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the Firewalls that have their configurations changed frequently.
Top 10 Network Devices with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the network devices that have their configurations changed frequently.
Top 10 Network IDSs with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the NIDSs that have their configurations changed frequently.
Top 10 Network Routings with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the network routings equipment that have their configurations changed frequently.
Top 10 Operating Systems Configuration Modifications Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks the top 10 OS configuration modifications.

Resource	Type	URI	Description
Top 10 Operating Systems with Configuration Modifications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Provides a list of the Firewalls that have their configurations changed frequently.
Last 10 Malware Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows the last 10 Malware Activity events.
Malicious Code Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows the malicious code activity between Attacker-Target pairs.
Top 10 Malwares	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Provides a list of the top 10 malware activity.
Anti-Virus Stopped or Paused	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the last state of systems that have had Anti-Virus services stopped or paused.
Last 10 Anti-Virus Service Stopped or Paused Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the last 10 Anti-Virus service stopped, paused, or disabled events.
Last 10 Failed Anti-Virus Updates	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the last 20 Anti-Virus service stopped, paused, or disabled events.
Last 10 Successful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a list of the last 10 successful logins by non-administrative users across your assets categorized in Network Domains.

Resource	Type	URI	Description
Last 10 Successful User Logouts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a list of the last 10 successful non-administrative user logouts across your assets categorized in Network Domains.
Last 20 Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a list of the last 20 unsuccessful non-administrative user logins across your assets categorized in Network Domains.
Last 20 User Login Attempts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows in real-time the last 20 login attempts for non-administrative users across your assets categorized in Network Domains.
Top 10 Hosts with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides an ordered list of hosts that most frequently have login failures for non-administrative users.
Top 10 Network Domains with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides an ordered list of the Network Domains that most frequently have non-administrative user login failures.
Top 10 Users with Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides an ordered list of non-administrative users who most frequently have failed logins.
Top User Login Activity	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the top 20 non-administrative users attempting to login to a system.
Unsuccessful User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Reports on a moving average of the number of unsuccessful user logins.

Resource	Type	URI	Description
User Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Reports on a moving average of the number of user logins.
Audit Log Cleared Status	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Reports violation suspected status when an audit log cleared event is present.
Last 20 Audit Log Cleared Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Reports the last 10 audit log cleared events.
Last 10 Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.
Last 10 Successful Administrative Logouts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the last 10 administrative logouts across your assets categorized in Network Domains.
Last 20 Unsuccessful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.
Top 10 Administrative Users with Successful Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the administrative attacker and target user name pairs with most successful logins
Top 10 Administrative Users with Unsuccessful Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the administrative attacker and target user name pairs with most failed logins

Resource	Type	URI	Description
Top 10 Hosts with Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the hosts with most successful administrative logins.
Top 10 Hosts with Unsuccessful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a list of the hosts with most unsuccessful administrative logins.
Top 10 Network Domains with Successful Administrative Logins	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides an ordered list of the Network Domains with most successful administrative logins.
Last 10 Security Patch Missing Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Displays in real-time the last 20 vulnerabilities related to IT Governance assets.
Top 10 Assets missing Security Patches	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows real-time display of the top 10 assets with security patches missing.
Last 20 Overflow Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides real-time display of the last 20 overflow vulnerabilities.
Last 20 SQL Injection Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides real-time display of the last 20 SQL vulnerabilities.
Last 20 Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the last 20 vulnerabilities.

Resource	Type	URI	Description
Last 20 Vulnerabilities with High CVSS	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the last 20 vulnerabilities with CVSS equal or higher than 8.
Last 20 XSRF Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides real-time display of the last 20 XSRF vulnerabilities.
Last 20 XSS Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides real-time display of the last 20 XSS vulnerabilities.
Last State Vulnerability Overview	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the last 20 vulnerabilities related to assets and their compliance status.
Top 10 Assets with Critical Vulnerabilities	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with critical vulnerability events.
Top 10 Overflow Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with vulnerability events.
Top 10 SQL Injection Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with vulnerability events.

Resource	Type	URI	Description
Top 10 Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with vulnerability events.
Top 10 XSRF Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with XSRF vulnerability events.
Top 10 XSS Vulnerable Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows real-time display of the top 10 assets with XSS vulnerability events.
Last 20 Peer to Peer Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the last 20 peer-to-peer events.
Peer to Peer Bandwidth Consumption per Port	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the total bandwidth consumption per port used in peer-to-peer traffic.
Peer to Peer Ports	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows all the ports involved in peer-to-peer traffic.
Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Detects non-ArcSight configuration modifications events.

Resource	Type	URI	Description
Database Configuration Modification	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Defines database configuration modifications.
Firewall Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks events when the configuration of a firewall is changed.
Network Device Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks events when the configuration of an infrastructural equipment (router, switch) is changed.
Network IDS Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks events when the configuration of NIDS equipment is changed.
Network Routing Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Tracks events when a modification to the routing table of infrastructural equipment (router, switch) is made.
Successful Modifications to Operating Systems	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Identifies successful configuration modifications to operating systems.
VPN Configuration Modifications	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects events indicating that a VPN configuration change has occurred.

Resource	Type	URI	Description
Windows Domain Policy Changed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects events indicating that a Windows domain policy was changed.
Windows Group Policy Changed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Selects events indicating that a Windows group policy was changed.
Resource Exhaustion	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).
Anti-Virus Clean or Quarantine Attempt	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects anti-virus events that indicate a quarantine or cleaning attempt of a detected malware instance.
Failed Virus Removal Attempt	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects events when an attempt to remove/quarantine a virus on a host failed.
Malicious Code Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects events where malicious code activity is detected.
Malware Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Identifies virus and other malware activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Potential Trojan Inside Network	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects events where a trojan is likely to be present inside the company network.

Resource	Type	URI	Description
Spyware Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Identifies spyware activity reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Trojan Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Selects events where trojan activity is detected.
Virus Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Identifies virus activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Worm Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Identifies worm activities reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Anti-Virus Service Stopped or Paused	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Selects events when an attempt to update a virus signature on a host failed.
Audit Log Cleared	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log 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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Detects correlated events the rule Audit Log Cleared generates

Resource	Type	URI	Description
Big Difference Between End Time and Manager Receipt Time	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronization/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronization/	Identifies different kinds of clock synchronization issues.
Device Time is Later than Agent Time	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronization/	Identifies 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.
Security Patch Missing	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Selects events indicating that a security patch is missing.
Software Changes	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Detects all changes to any software installed.
Critical Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events indicating that a critical vulnerability was detected.
Exploit of Vulnerability	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events where an attempt at exploiting a vulnerability is detected.
Overflow Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events indicating that an overflow vulnerability detected.

Resource	Type	URI	Description
SQL Injection Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events indicating that SQL injection vulnerability was detected.
XSRF Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events indicating that an XSRF vulnerability was detected.
XSS Vulnerability Detected	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Selects events indicating that an XSS vulnerability was detected.
Peer to Peer Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Identifies peer-to-peer traffic.
Windows Scheduled tasks Created	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Selects Windows scheduled tasks created events.
Windows Services Installed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Selects Windows service installed events.
Information System Audit Tool Login	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.7 Information systems audit considerations/12.7.1 Information systems audit controls/	Identifies logins to information system audit tools. By default it shows only logins to ArcSight products.

Resource	Type	URI	Description
Resource Exhaustion Detected on Operations	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on operations domain.
Resource Exhaustion Detected on Processing Systems	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on processing systems.
Resource Exhaustion Detected on Production	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	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	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	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 Systems	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on third party systems.
Top 10 Vulnerable Assets - Production	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable assets on production.
Top 10 Vulnerable Assets - Public Facing	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable assets on public facing.

Resource	Type	URI	Description
Top 10 Vulnerable Assets - Third Party	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable assets on Third Party.
Configuration Changes - Trend Base	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Retrieves all configuration changes for the last hour and used as trend base query for the Configuration Changes trend.
Firewall Configuration Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows any configuration modifications of any firewall. Default time window: Last 24 hours.
Firewall Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top configuration modifications of any firewall.
Network Device Configuration Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows any configuration modifications of any network equipment.
Network Device Configuration Modifications by Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top configuration modifications of network equipment.
Network Routing Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows all router configuration modifications.

Resource	Type	URI	Description
Network Routing Changes by Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top router configuration modifications.
Successful Changes to Operating Systems	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the number of times changes were made to operating systems.
Successful Database Configuration Modification	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows all events on database configuration modifications.
Top Firewalls with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top firewalls with most successful configuration modifications.
Top Network Devices with Most Successful Configuration Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top network devices with most successful configuration modifications.
Top Network Devices with Most Successful Network Routing Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows top routers/switches with most successful routing configuration modifications.
Top Users with Most Successful Firewall Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top users who made most successful configuration modifications.

Resource	Type	URI	Description
Top Users with Most Successful Network Devices Configuration Modifications	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top users with most successful configuration modifications.
Weekly Trend - Configuration Changes by Address	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top configuration modifications by IP address.
Weekly Trend - Configuration Changes by Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top configuration modifications.
Weekly Trend - Configuration Changes by User	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top configuration modifications by user.
Windows Domain Policy Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Lists all the changes to Microsoft Domain Policy.
Windows Group Policy Changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Lists all the changes to Microsoft Active Directory.
Resource Exhaustion Detected	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes).

Resource	Type	URI	Description
Resource Exhaustion Detected - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain).
Detected Malware Summary by Hosts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows a summary of malware detected on systems sorted by host.
Malicious Code Activities from Internal Sources	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows all malicious code activities from internal sources.
Top External Sources with Malicious Code Activities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows the top external sources with most malicious code activities.
Top Hosts with Most Malware Activities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Finds the top 10 systems with the most malware activities (routine maintenance and remediation events).
Top Hosts with Most Spyware Activities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	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/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows the top hosts with most virus activities detected on systems.
Top Internal Sources with Malicious Code Activities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows the top internal sources with most malicious code activities.

Resource	Type	URI	Description
Top Malware Instances	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Provides the names of the top 10 detected malware instances.
Top Spyware Instances	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Provides the names of the top 10 detected spyware instances.
Top Virus Instances	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows a summary of virus activities detected on systems sorted by virus.
Worm Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows all worm activity.
All User Logins per User	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a listing of user logins per user name.
Anti-Virus Stopped or Paused in the Last Month	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows all events when an anti-virus service is stopped or paused in the last month.
Daily Anti-Virus Stopped or Paused - Trend Base	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows all events when an anti-virus service is stopped or paused on systems.
Daily Count of Successful User Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Retrieves 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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Counts the number of unsuccessful daily user logins.

Resource	Type	URI	Description
Failed Anti-Virus Updates	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows all the failed Anti-Virus updates on systems.
Number of Daily User Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Captures the number of logins per user and outcome over the entire day.
Successful User Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows details of all successful user logins within the last day.
Successful User Logins by Hour	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Retrieves the number of non-administrative successful user logins per hour.
Unsuccessful User Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows details of all unsuccessful user logins within the last day.
Unsuccessful User Logins by Hour	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Retrieves the number of non-administrative successful user logins per hour.
User Local Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows details of local login events to a MS Windows or UNIX system.
User Logins and Logouts	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows details of user logins and logouts within the last day.
Audit Log Cleared	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log 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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows the number of times an audit log was cleared by an attacker user name.

Resource	Type	URI	Description
Audit Log Cleared per Attacker and Target	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows the number of times audit logs were cleared from a host by an attacker
Audit Log Cleared per Target User Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows the number of times an audit log was cleared by a target user name.
Syslog Restart Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all restarts of syslog on systems.
Windows System audit policy changes	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all Windows system audit policy changes.
Administrative Logins and Logouts per User	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a listing of administrative logins and logouts per user name.
Count of Administrative Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows details of all successful administrative logins within the last 30 days.
Count of Successful Administrative Logins in the Last 30 days	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows a count of unsuccessful administrative logins within the last 30 days.

Resource	Type	URI	Description
Daily Successful Administrative Logins per Hour	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows the hourly number of successful administrative logins.
Daily Unsuccessful Administrative Logins per Hour	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows the hourly number of unsuccessful administrative logins.
Number of Successful Administrative Logins by User and Host Information	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	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. May be focused based on the Network Domain of interest.
Successful Administrative Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows details of all successful Administrative logins within the last day.
Top 10 Hosts with Most Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Returns the top 10 hosts with most unsuccessful login attempts within the last 2 hours. May (and should) be focused based on the Network Domain of interest.
Trend of Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows the trend of unsuccessful administrative logins over long term.
Unsuccessful Administrative Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows details of all unsuccessful administrative logins within the last day.

Resource	Type	URI	Description
Unsuccessful Administrative Logins - Long Term Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Counts the number of failed administrative logins per attacker user name, target user name and target address per month.
Unsuccessful Administrative Logins in the Last 2 Hours	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows details of all unsuccessful administrative logins within the last 2 hours.
Clock Synchronization Issues	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronisation/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronisation/	Displays a summary of the number of events for each device that had clock synchronization issues.
Application Configuration Modifications on Operations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows any configuration modifications of any application on operations. Default time window: Last 24 hours.
Missing Security Patches Summary	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Provides overview of the missing security patches summary.
Software Changes in Operations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows all changes to any software installed in the operations network segment.
CVSS Score Greater than or Equal to 8	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows vulnerabilities with CVSS >=8.

Resource	Type	URI	Description
Exploit of Vulnerability	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows all incidents of attempts to exploit vulnerabilities in an application.
Overflow Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows overflow vulnerabilities identified on the last 24 hours.
SQL Injection Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows SQL injection vulnerabilities identified on the last 24 hours.
Top 10 Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerabilities on IT Governance Assets.
Top 10 Vulnerable Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable IT Governance assets.
Top 10 Vulnerable Assets on Network Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable Assets by network domain (default Development)
Top Critical Vulnerabilities - on Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Retrieves the top 20 critical vulnerabilities for the last 14 days.

Resource	Type	URI	Description
Top Vulnerable IP Addresses	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Retrieves the top 10 vulnerable IP Addresses for the last 14 days.
Vulnerabilities - Trend Base	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	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/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Retrieves all the vulnerabilities for the last 14 days.
Vulnerabilities Summary	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of the vulnerability summary on IT Governance Assets.
Vulnerabilities by IP Address - on Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Retrieves all the vulnerabilities for the last 14 days for specific IP Address.
Vulnerability Events By Scanner - on Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows vulnerability count per scanner for the last 14 days.
Vulnerability Scans - on Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows all the vulnerability scans for the last 14 days.

Resource	Type	URI	Description
XSRF Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows XSRF vulnerabilities identified on the last 24 hours.
XSS Vulnerabilities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows XSS vulnerabilities identified on the last 24 hours.
Peer to Peer Internal Sources	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the most common sources for peer-to-peer applications.
Peer to Peer Traffic	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the most common peer-to-peer traffic.
Services by Host Name	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Returns all unencrypted services by a particular host name identified in the last 24 hours using vulnerability and port scanning events.
Windows Scheduled Tasks Created	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows all Windows scheduled tasks created.
Windows Services Installed	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows all Windows services installed.

Resource	Type	URI	Description
Information System Audit Tool Logins	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.7 Information systems audit considerations/12.7.1 Information systems audit controls/	Shows logins, both successes and failed, to information system audit tools.
Count of Successful Administrative Logins in the Last 30 Days	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows a count of successful administrative logins in the last 30 days, ordered by the most occurring logins.
Count of Unsuccessful Administrative Logins in the Last 30 Days	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows a count of unsuccessful administrative logins in the last 30 days, ordered by the most occurring failures.
Top 10 Hosts with Most Unsuccessful Administrative Logins in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows top 10 hosts with most unsuccessful administrative logins in the last 2 hours. Provides drill-downs by host name to detailed info about host's unsuccessful administrative logins.
Unsuccessful Administrative Logins in the Last 2 Hours	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows details of all unsuccessful administrative logins in the last 2 hours. Provides drill-downs into various fields.
Top Critical Vulnerabilities	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows summary of top critical vulnerabilities, where the user can drill down to detailed information about those vulnerabilities.
Top Vulnerable IP Addresses	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows top vulnerable IP addresses in bar chart format.
Vulnerabilities	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows all the vulnerabilities.

Resource	Type	URI	Description
Vulnerability Events By Scanner	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows vulnerability events count for each scanner.
Vulnerability Scans	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	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.
Database Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows database configuration changes.
Firewall Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows several top-level views related to firewall configuration modifications.
List of Firewall Configuration Modifications	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows any configuration modifications of any firewall.
List of Network Device Configuration Modifications	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows any configuration modifications of any network equipment. Default time window: Last 24 hours.
List of Network Routing Modifications	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows all router configuration modifications.

Resource	Type	URI	Description
Network Device Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows several top-level views of configuration modifications of any network equipment.
Network Routing Modification Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows the top routers with routing configuration modifications, and top routing modifications.
Successful Changes to Operating Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays the number of times changes were made to operating systems.
Weekly Trend - Configuration Modification Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Shows several top-level views related to firewall configuration modifications.
Windows Domain Policy Changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays changes to Microsoft Domain Policy for the last 24 hours.
Windows Group Policy Changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Displays changes to Microsoft Active Directory for the last 24 hours.
Resource Exhaustion Detected	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes).

Resource	Type	URI	Description
Resource Exhaustion Detected on Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.3 Capacity management/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on network domain (default development domain).
Malicious Code Sources	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows information about the sources of malicious code activities.
Malware Activities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows an overview of malware activities.
Malware Activity Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows a summary of virus activities detected on systems, sorted by host.
Spyware Activities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows an overview of spyware activities.
Virus Activities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows a summary of virus activities detected on systems sorted by virus.
Worm Activity Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.2 Protection from malware/12.2.1 Controls against malware/	Shows a summary of worm activities detected on systems, sorted by host.
All User Logins per User	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a listing of all logins for a particular user.

Resource	Type	URI	Description
Anti-Virus Stopped or Paused in the Last Month	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows all events when Anti-Virus is stopped or paused in the last month.
Daily Successful User Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a listing of successful user login attempts.
Daily Unsuccessful User Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a listing of unsuccessful user login attempts.
Daily User Logins and Logouts	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Provides a listing of user logins and logouts events.
Failed Anti-Virus Updates	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows all the failed Anti-Virus updates.
Number of Successful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the number of successful user logins every day over the past week.
Number of Successful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the number of successful user logins per hour.
Number of Unsuccessful User Logins over the Past Month	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the number of unsuccessful user logins every day over the past month.
Number of Unsuccessful User Logins over the Past Week	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the number of unsuccessful user logins every day over the past week.

Resource	Type	URI	Description
Number of Unsuccessful User Logins per Hour over the Past Day	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows the number of unsuccessful user logins every hour over the past day.
User Local Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Shows local login events to a MS Windows or UNIX system.
Audit Log Cleared	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all events where an audit log was cleared from a host.
Audit Log Cleared per Attacker User Name	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all events where an audit log was cleared by an attacker user name.
Audit Log Cleared per Attacker and Target	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all events where audit logs were cleared from a host by an attacker
Audit Log Cleared per Target User Name	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all events where an audit log was cleared by a target user name.
Syslog Restart Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all restarts of syslog on systems.
Windows System audit policy changes	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Shows all Microsoft system audit policy changes.

Resource	Type	URI	Description
Administrative Logins and Logouts per User	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a listing of administrative logins and logouts per target or attacker user name.
Daily Successful Administrative Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a listing of successful administrative login attempts.
Daily Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Provides a listing of unsuccessful administrative login attempts.
Monthly Trend of Unsuccessful Administrative Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows different aspects of the trend of unsuccessful administrative logins in the last 16 weeks.
Number of Successful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows the hourly number of successful administrative logins and a list of those logins, grouped by user and host information.
Number of Unsuccessful Administrative Logins by User and Host	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Shows the hourly number of unsuccessful administrative logins, and a listing of those attempts, grouped by user and host information.
Clock Synchronization Issues	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronisation/	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/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.4 Clock synchronisation/	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.

Resource	Type	URI	Description
Application Configuration Modifications on Operations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows any configuration modifications of any application on a system on operations. Default time window: Last 24 hours.
Missing Security Patches Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows missing security patches summary. Default time window: Last 24 hours.
Software Changes in Operations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Shows any configuration modifications of any application on a system on operations. Default time window: Last 24 hours.
CVSS Score Greater than or Equal to 8 Overview	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of vulnerabilities with CVSS >=8 on the last 24 hours.
Exploit of Vulnerability	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows all incidents of attempts to exploit vulnerabilities in an application. The report is sorted first by the outcome of the attempts and then by the number of events.
Overflow Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows overflow vulnerabilities identified on the last 24 hours.
SQL Injection Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows SQL injection vulnerabilities identified on the last 24 hours.

Resource	Type	URI	Description
Top 10 Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerabilities on IT Governance assets.
Top 10 Vulnerable Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable IT Governance assets.
Top 10 Vulnerable Assets on Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows the top 10 vulnerable IT assets on network domain (default Development Network Domain)
Vulnerabilities by IP Address	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Displays vulnerability overview by IP Address for the last 14 days (default 127.0.0.1).
Vulnerability Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Provides overview of the vulnerability summary in the last 24 hours.
XSRF Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows XSRF vulnerabilities identified on the last 24 hours.
XSS Vulnerabilities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Shows XSS vulnerabilities identified on the last 24 hours.

Resource	Type	URI	Description
Peer to Peer Internal Sources	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the most common machines within the network involved in peer-to-peer traffic, the number of unique peers communicated with and the total number of peer-to-peer events.
Peer to Peer Traffic	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows the most common peer-to-peer traffic.
Services by Host Name	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Returns all services by a particular host name (by default localhost) identified in the last 24 hours using vulnerability and port scanning events.
Windows Scheduled Tasks Created	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows all Windows scheduled tasks created.
Windows Services Installed	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.2 Restrictions on software installation/	Shows all installed Windows services and the time of the installation.
Information System Audit Tool Logins	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.7 Information systems audit considerations/12.7.1 Information systems audit controls/	Shows logins, both successful and failed, to information system audit tools.

Resource	Type	URI	Description
Critical Network Device Configuration Change Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	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/IT Governance/ISO 12 Operation Security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Triggers when operating system change is detected on critical asset and has Very-High agent severity.
Malware or Spyware Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.2 Protection from malware/12.2.1 Controls against malware/	Triggers when a spyware or malware activity is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Suspicious Internal Trojan Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.2 Protection from malware/12.2.1 Controls against malware/	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/IT Governance/ISO 12 Operation Security/12.2 Protection from malware/12.2.1 Controls against malware/	Triggers when a worm is reported by either an Intrusion Detection System (IDS) or an anti-virus application.
Security Software Stopped or Paused	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.4 Logging and monitoring/12.4.1 Event logging/	Triggers when a security software service has been disabled.
Audit Log Cleared	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.4 Logging and monitoring/12.4.2 Protection of log information/	Monitors for events on clearing of the audit log on Windows systems.

Resource	Type	URI	Description
Consecutive Unsuccessful Logins to Administrative Account	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Fires when it notices a set of 10 consecutive unsuccessful logins by an attacker and target user name pair within 5 minutes.
Unsuccessful Logins to Multiple Administrative Accounts	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Fires when it notices a set of 20 continuous unsuccessful logins by different administrative attacker and target user pairs within 5 minutes.
Security Patch Missing	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.5 Control of operational software/12.5.1 Installation of software on operational systems/	Triggers when a security patch missing vulnerability is detected.
Critical Vulnerability Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when a critical vulnerability is detected.
Overflow Vulnerabilities	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when an overflow vulnerability is detected.
SQL Injection Vulnerabilities	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when SQL Injection vulnerability is detected.
Vulnerabilities on Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when a vulnerability is detected on critical machine.

Resource	Type	URI	Description
XSRF Vulnerabilities	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when XSRF vulnerability is detected.
XSS Vulnerabilities	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 12 Operation Security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Triggers when XSS vulnerability is detected.
Configuration Changes	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.1 Operational procedures and responsibilities/12.1.2 Change management/	Collects hourly data using the Configuration Changes Trend Base query. Used by other queries to show configuration changes.
Daily Trend of Anti-Virus Stopped or Paused Events	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Stores all events when an Anti-Virus service is stopped or paused.
User Login Count	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.1 Event logging/	Stores a daily count of user login attempts.
Count of Administrative Logins	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Stores a count of successful and unsuccessful administrative logins.
Failed Administrative Logins - Long Term Trend	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.4 Logging and monitoring/12.4.3 Administrator and operator logs/	Stores long term information about failed administrative logins.
Vulnerabilities	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 12 Operations security/12.6 Technical vulnerability management/12.6.1 Management of technical vulnerabilities/	Collects hourly data using the Vulnerabilities trend Base query.

ISO 13: Communication Security Resources

Resource	Type	URI	Description
Firewall Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the Firewall category device group.
IDS Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the IDS category device group.
Network Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the Network category device group.
VPN Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the VPN category device group.
Traffic Between Network Domains	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows all the traffic between network domains.
Information Interception	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows events that represent a possible interception of data over a 2 hour continuously sliding window.

Resource	Type	URI	Description
DoS Attacks	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows events that are attributed to denial of service attacks.
All Information Leak Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows real-time feed of events reflecting information leakage.
Network Controls	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Displays information about logging devices and firewall open ports.
Traffic Between Network Domains	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Displays information about traffic between network domains.
Blocked Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows information related to blocked traffic activity.
Information Interception	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Displays information about interception events.
Traffic Anomaly	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Displays information about traffic anomaly events.

Resource	Type	URI	Description
DoS Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Provides an overview of events associated with denial of service and availability attacks.
IM Traffic	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Displays information around Instant Messaging traffic and sources.
Spam Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Displays information about spam events.
Information Leaks	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Displays information around information leakage.
Firewall Open Ports	Data Monitor	U	Used to determine which ports a particular firewall is allowing traffic on.
Logging Devices	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows all devices that are sending their logs.
Internal Inter-Domain Traffic by Attacker Domain	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows the internal inter-domain traffic by attacker domain.
Internal Inter-Domain Traffic by Target Domain	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows the internal inter-domain traffic by target domain.

Resource	Type	URI	Description
Last 10 Internal Inter-Domain Traffic	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Displays the last 10 Internal Inter-Domain Traffic.
Top Internal Inter-Domain Communications	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows the top attacker and target domain pairs with most traffic.
Blocked Traffic	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	This data monitor presenting blocked traffic in event graph chart.
Last 10 Blocked Traffic Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows the last 10 blocked traffic events.
Last 10 Information Interception Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows the last 10 Information Interception events.
Last 10 Traffic Anomaly Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows the last 10 Traffic Anomaly events.
Top Blocked Traffic Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Displays a bar chart of the top attacker addresses of blocked traffic.

Resource	Type	URI	Description
Top Information Interception Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Displays a bar chart of the attacker addresses and priorities for information interception events.
Top Traffic Anomaly Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Provides a list of the top 10 anomaly traffic per Attacker and Target addresses.
Traffic Anomaly	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Presents traffic anomalies in an event graph chart.
Traffic Anomaly by Protocol	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Provides the distribution of traffic anomaly by protocol.
DoS Attacks Event Names - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows connections between attacker and target machines and event names as they appear in denial of service attack events
DoS Attacks Event Ports - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows connection between attacker and target machines and ports as they appear in denial of service attack events.
Last 10 Spam Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Displays the last 20 spam events.
Last 20 DoS Attack Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Displays the last 20 denial of service attack events.

Resource	Type	URI	Description
Last 50 IM Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the last 50 Instant Messaging events.
Top 10 DoS Attackers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top 10 DoS Attackers.
Top 10 DoS Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top 10 DoS targets.
Top 10 Spam Receivers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top 10 spam targets.
Top 10 Spammers	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top 10 spammers.
Top IM Services	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top Instant Messaging services.
Top IM Sources	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top Instant Messaging sources.
Organizational Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Displays a graph with events which pertain to information leaks of organizational records.

Resource	Type	URI	Description
Personal Information Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows communications pertaining to personal information leaks.
Firewall Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the Firewall category device group.
IDS Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Retrieves events with the IDS category device group.
Network Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Identifies events with the category object starts with Network or the category device group starts with Network Equipment.
VPN Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Identifies events in which the category device group is VPN.
Access Attempts	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Identifies access attempts other than logins.
Internal Inter-Domain Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Identifies internal inter-domain traffic.

Resource	Type	URI	Description
Successful Access	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Identifies successful access other than logins. E.g. database query.
Traffic Between Network Zones	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Detects events in which the attacker zone is different than the target zone.
Covert Channel	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating a covert channel is being used.
External to Internal Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects events where the traffic originates from external network segment and the target is in an internal network segment.
Information Interception	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating an information interception is being used.
Internal to External Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects events where the traffic originates from an internal network segment and the target is in an external network segment.
Redirection Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating a redirection attack occurred.

Resource	Type	URI	Description
Traffic Anomaly	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating a traffic anomaly.
Traffic Anomaly on Application Layer	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating a traffic anomaly on application layer
Traffic Anomaly on Network Layer	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events indicating traffic anomaly in transport layer.
Traffic from Dark Address Space	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events that are coming from the Dark Address Space.
Traffic to Dark Address Space	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Detects events that are targeting the Dark Address Space.
DoS Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Identifies denial of service attacks.

Resource	Type	URI	Description
Email Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Detects events indicating an email attack occurred.
Email Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Identifies generic email traffic.
IM Traffic	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Identifies all instant messaging traffic that are not supposed to be allowed.
Phishing Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Detects events indicating a phishing attack occurred.
Spamming Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Detects events indicating an email spam sent.
Successful DoS Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Identifies successful denial of service attacks.
Unsuccessful and Attempted DoS Attacks	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Identifies unsuccessful and attempted denial of service attacks.
All Information Leak Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Selects events that reflect information leakage.

Resource	Type	URI	Description
Organizational Records Information Leak	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Identifies information leaks with regard to company information.
Personal Information Leak	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Selects events which indicate a personal information leak.
Blocked Firewall Traffic from Assets in Partner Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	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 Partner Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	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 Partner Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	This report provides a listing of the outbound firewall traffic originating from assets in the partner domain.
Firewall Traffic to Assets in Partner Domain	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	This report provides a listing of the inbound firewall traffic directed to assets in the partner Domain.
Device Logging Review	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows the different products that are logging to ArcSight ESM.

Resource	Type	URI	Description
Events per Device	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows the number of events reported each device over the past day.
Open Firewall Port Details	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Gives details of all the ports that are allowed to pass through various firewalls.
Open Firewall Port Summary	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Gives a summary of all the ports that are allowed to pass through firewalls.
Access to Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows all successful accesses to systems in a certain Network Domain.
Cross Talk between 2 Network Domains	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Provides the cross-talk in the last 24 hours between assets in Development category and assets in Test category.
Suspicious Activity on Network Domains from Machines not in that Domain	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	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/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows the target ports between zones.

Resource	Type	URI	Description
Blocked Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	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/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Covert Channel Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all covert channel activity.
External to Internal Traffic	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	This query counts all events from external to internal sources per device and source-target pair. The query runs over the last 24 hours.
Firewall Traffic from Assets - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	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/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Provides a listing of the inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Information Interception Activity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all covert channel activity.

Resource	Type	URI	Description
Internal to External Traffic	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	This query counts all events from internal to external sources per device and source-target pair. The query runs over the last 24 hours.
Redirection Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all redirection attacks.
Traffic Anomaly on Application Layer	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on network layer.
Traffic Anomaly on Transport Layer	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on transport layer.
Traffic from Dark Address Space	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic to Dark Address Space	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all traffic directed to a dark address range. This should be considered very suspicious.

Resource	Type	URI	Description
External Traffic to Internal Domain - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	This query counts all events from external sources to internal domain to per device and source-target pair. The query runs over the last 24 hours.
Internal Domain to External Traffic - Template	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	This query counts all events from internal domain to external sources per device and source-target pair. The query runs over the last 24 hours.
Count of DoS Attacks per Day	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	This query counts the total number of weekly denial of service attack events.
DoS Attacks Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	This query summarizes the number of DoS attacks for long term reporting.
DoS Attacks by Attacker	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Provides a weekly count of attacker addresses appearing in DoS attack events.
DoS Attacks by Target	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Provides a weekly count of target addresses appearing in DoS attack events.
Email Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email attacks.
External Hosts Receiving Most IM Traffic	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows top external hosts receiving most Instant Messaging traffic.

Resource	Type	URI	Description
Internal IM Sender	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows internal hosts with outgoing (not necessarily outbound) Instant Messaging traffic.
Most Popular IM Traffic Ports	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the most common Instant Messaging target ports.
Most Popular IM Traffic Services	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the most common Instant Messaging services.
Phishing Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email attacks.
Ports and Events for DoS Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the various ports and events used in denial of service attacks.
Spam per Hour	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	This query gets the number of spam emails sent every hour over the past day.
Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the details of successful denial of service attacks.
Target Object in Successful DoS Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the number of times a particular object has been a victim of denial of service attacks.

Resource	Type	URI	Description
Target Object in Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	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/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top attackers responsible for initiating denial of service attacks.
Top DoS Targets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows hosts which were targeted the most with denial of service attacks.
Top Email Receivers by Email Size	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top email recipients based on the size of emails received.
Top Email Receivers by Number of Emails	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top email recipients based on the number of emails received.
Top Email Senders by Email Size	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top email senders based on the size of emails sent.
Top Email Senders by Number of Emails	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top email senders based on the number of emails sent.
Top Phishing Email Receivers	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top phishing email recipients.

Resource	Type	URI	Description
Top Phishing Email Senders	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top phishing email senders.
Top Spam Receivers	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top phishing email recipients.
Top Spam Senders	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the top phishing email senders.
Unsuccessful and Attempted DoS Attacks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the details of unsuccessful and attempted denial of service attacks.
All Information Leaks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows all activity flagged as information leakage.
Organizational Records Information Leaks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows communications which were classified as information leaks of organizational records.
Organizational Records Information Leaks on Financial Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows communications which were classified as information leaks of financial organizational records originated from third-party assets.
Organizational Information Leaks Originated from Third Party	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows events which indicate a personal information leak originated from third-party assets.

Resource	Type	URI	Description
Personal Information Leaks	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows events which indicate a personal information leak.
Personal Information Leaks Originated from Third Party	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows events which indicate a personal information leak originated from third-party assets.
Events per Device	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows the number of events that have been reported by a particular device over the past day.
Logging Devices	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows the different products that are logging to ArcSight ESM.
Open Firewall Port Summary	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	This query viewer gives a summary of all the ports that are allowed to pass through various firewalls.
Ports and Events for DoS Attacks	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows the various ports and events used in denial of service attacks.
Device Logging Review	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	Shows the different products that are logging to ArcSight ESM.

Resource	Type	URI	Description
Open Firewall Port Details	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.1 Network controls/	This report gives details of all the ports that are allowed to pass through various firewalls.
Access to Network Domains from Machines not in that Domain	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows all successful access attempts to systems in a particular Network Domain from systems not in that domain.
Cross-Talk Between Network Domains - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows all cross-talk in the last 24 hours between assets in 2 network domains. Default network domains: development and test.
Suspicious Activity on Network Domains from Machines not in that Domain	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows all suspicious activity to systems in a particular Network Domain from systems not in that domain.
Traffic Between Zones	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.1 Network security management/13.1.3 Segregation in networks/	Shows the target ports between zones.
Blocked Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	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/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	This report provides a listing of the blocked inbound firewall traffic directed at assets in the indicated Network Domain of interest.

Resource	Type	URI	Description
Covert Channel Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all covert channel activity.
Firewall Traffic from Assets in Network Domain - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	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/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	This report provides a listing of the inbound firewall traffic directed at assets in the indicated Network Domain of interest.
Information Interception Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all information interception activity.
Redirection Attacks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all redirection attacks
Traffic Anomaly on Application Layer	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on application layer.
Traffic Anomaly on Network Layer	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on network layer.

Resource	Type	URI	Description
Traffic Anomaly on Transport Layer	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows traffic anomaly on transport layer.
Traffic Between Internal and External Sources - All	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows two tables. The first showing a count of events representing traffic from internal to external sources. The second table shows a count of events representing traffic from external to internal sources. The count is shown for each source-destination pair and for each device.
Traffic Coming from Dark Address Space	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all traffic from a dark address range targeting systems. This should be considered very suspicious.
Traffic to Dark Address Space	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Shows all traffic directed to a dark address range. This should be considered very suspicious.
External to Internal Domain Traffic - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	Counts all events from external sources to internal Domain (default Development Domain) per device and source-target pair. The query runs over the last 24 hours.
Internal Domain to External Traffic - Template	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.2 Agreements on information transfer/	This report counts all events from internal domain (default Development Domain) to external sources per device and source-target pair. The query runs over the last 24 hours.
DoS Attacks Weekly Trend	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Displays a weekly overview of DoS attack events.

Resource	Type	URI	Description
Email Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email activity in the last day.
Email Attacks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email attacks
IM Traffic Summary	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows several high-level views of Instant Messaging traffic.
Internal IM Senders	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows several high-level views of internal Instant Messaging senders.
Phishing Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email phishing activity in the last day.
Spam Activity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows all email spam activity in the last day.
Successful DoS Attacks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows details of successful denial of service attacks.
Unsuccessful and Attempted DoS Attacks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows details of unsuccessful and attempted denial of service attacks.

Resource	Type	URI	Description
All Information Leaks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows all activity that was flagged as information leakage.
Organizational Records Information Leaks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows the communications which were classified as information leaks of organizational records.
Organizational Records Information Leaks Originated from Third-Party	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows the communications which were classified as information leaks of organizational records originated from third party.
Organizational Records Information Leaks on Financial Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows the communications which were classified as information leaks of organizational records on financial assets.
Personal Information Leaks	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows events which indicate a personal information leak.
Personal Information Leaks Originated from Third-Party	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Shows events which indicate a personal information leak originated from third party.
Top DoS Attackers	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows a list of top attackers responsible for initiating denial of service attacks.

Resource	Type	URI	Description
Top DoS Targets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Shows hosts which were targeted the most with a denial of service attack.
Communication between Production and Development Domains	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.1 Network security management/13.1.3 Segregation in networks/	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/IT Governance/ISO 13 Communication Security/13.1 Network security management/13.1.3 Segregation in networks/	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/IT Governance/ISO 13 Communication Security/13.1 Network security management/13.1.3 Segregation in networks/	Fires any time communication between a sensitive asset and a machine in the Third Party domain is detected.
Possible Covert Channel	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects events indicating a covert channel is being used.
Possible Information Interception	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects attacks where information could be redirected and collected by an unintended party.
Possible Redirection Attack	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects attacks where information could be redirected.

Resource	Type	URI	Description
Possible Traffic Anomaly	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.1 Information transfer policies and procedures/	Selects attacks where information could be redirected and collected by an unintended party.
DoS Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.3 Electronic messaging/	Selects DoS.
Possible Email Attack	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.3 Electronic messaging/	Selects attacks where email activity involved.
Potential Distributed DoS	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.3 Electronic messaging/	Selects Potential Distributed DoS
Information Leak on HR assets	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Selects any HR organizational information being sent out of the corporate network.
Information Leak on of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 13 Communication Security/13.2 Information transfer/13.2.4 Confidentiality or nondisclosure agreements/	Selects any organizational information being sent out of the corporate network.
DoS Attacks Trend	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 13 Communications security/13.2 Information transfer/13.2.3 Electronic messaging/	Stores long term aggregated information about DoS attack events.

ISO 14: System Acquisition, Development and Maintenance Resources

Resource	Type	URI	Description
Invalid Input Data	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Provides overview of invalid input data on the organization.
Development Domain Traffic Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	This Dashboard provides overview of development domain traffic activity.
Development Login Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides overview of the login activity on the development domain.
Last 20 Invalid Input Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Real-time display of the last 20 Invalid Input Events.
Top 10 Assets with Invalid Input Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Real-time display of the top 10 assets with invalid input events.
Last 10 Successful Logins to Development	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.
Last 10 Traffic to Development from other Network Domains	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides the last 10 Traffic to development from other network Domains

Resource	Type	URI	Description
Last 10 Unsuccessful Logins to Development	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.
Top 10 Hosts with Successful Logins to Development	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides a list of the hosts with most successful administrative logins.
Top 10 Hosts with Unsuccessful Logins to Development	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides a list of the hosts with most unsuccessful administrative logins.
Top 10 Traffic to Development from other Network Domains	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	Provides the top 10 Traffic to Development from other Network Domains.
Driver Loaded	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where driver is loaded.
Driver Unloaded	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where driver is unloaded.
Module Loaded	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where Module is loaded.
Module Unloaded	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where Module is unloaded.

Resource	Type	URI	Description
Software Installed	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where software is installed.
Software Uninstalled	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Selects events where software is un-installed.
Invalid Data Input	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Selects events where invalid data input is detected.
Successful Logins to Development	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	This filter identified successful logins by both administrative and non-administrative users to development domain.
Unsuccessful Logins to Development	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.6 Secure development environment/	This filter identified unsuccessful logins by both administrative and non-administrative users to development domain.
Outsourced Development Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.7 Outsourced development/	This report provides a listing of all the outsourced development assets.
Changes to Software Packages on Critical Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Shows all changes to software packages on critical assets.
Invalid Data Input to Host	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Shows all incidents of invalid data input to a particular host.

Resource	Type	URI	Description
Logins and Logouts to Outsourced Development Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.7 Outsourced development/	Retrieves logins and logouts to outsourced development assets.
Suspicious Activity in Outsourced Development Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.7 Outsourced development/	Shows suspicious activities in the Outsourced Development Assets.
Changes to Software Packages on Critical Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	Shows all changes to software packages on critical assets on the last day.
Invalid Data Input to Host	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.5 Secure system engineering principles/	Shows all incidents of invalid data input to a particular IP.
Logins and Logouts to Outsourced Development Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.7 Outsourced development/	Lists all the logins and logouts to outsourced development assets on the last 24 hours.
Suspicious Activity in Outsourced Development Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.7 Outsourced development/	Shows suspicious activity by users on the outsourced development domain.
Module Loaded or Unloaded on Critical Asset	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 14 System acquisition, development and maintenance/14.2 Security in development and support processes/14.2.4 Restrictions on changes to software packages/	This rule triggers when a module is loaded or unloaded on critical asset.

ISO 15: Supplier Relationships Resources

Resource	Type	URI	Description
Attacks and Suspicious Activity Targeting Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all attack and suspicious activity events where the target is an asset from Third Party asset category.
Attacks and Suspicious Activity from Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all attack and suspicious activity events where the attacker is an asset from Third Party asset category.
Attacks and Suspicious Activity to and from Third Party Resources	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays information about third party assets involved in attacks and suspicious behavior.
Attacks and Suspicious Activity Events in the Third Party Network Domain - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows connection between source and destination machines and ports as they appear in attack and suspicious activity events in the Third Party Network Domain.
Last 20 Attacks and Suspicious Activity Events Targeting Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays the last 20 attack and suspicious activity events where the traffic originated from a Third Party asset or zone.

Resource	Type	URI	Description
Ports Used in Attacks and Suspicious Activity Events Targeting Third Party Resources	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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.
Attacks and Suspicious Activity Targeting Third Party Resources	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies attack and suspicious activity events targeting or originating from assets or zones categorized in the Third Party asset category.
Successful Administrative Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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.

Resource	Type	URI	Description
Successful User Logins from Third Party Systems	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Identifies 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.
Successful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Retrieves successful logins with an administrator account from assets categorized as Third Party.

Resource	Type	URI	Description
Successful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Retrieves successful logins using a non-administrative account, to assets categorized as Third Party.
Third-Party Access	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all access attempts to assets by third parties.
Third-Party Incidents - Closed Cases	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all cases involving third-party systems that have been closed.
Third-Party Incidents - Open Cases	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all cases involving third-party systems that are still open.
Unsuccessful Administrative Logins from Third Party Systems	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Retrieves failed logins using an administrative account, from assets categorized as Third Party.

Resource	Type	URI	Description
Unsuccessful Administrative Logins to Third Party Systems	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Retrieves failed logins with a non-administrator account to assets categorized as Third Party.
Successful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays all successful administrative logins from assets categorized as Third Party.
Successful Administrative Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays all successful non-administrative logins from assets categorized as Third Party.
Successful User Logins to Third Party Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays all successful non-administrative logins to assets categorized as Third Party.

Resource	Type	URI	Description
Third-Party Access	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all access attempts to third party assets.
Third-Party Incidents - Closed Cases	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all cases involving third-party systems that have been closed.
Third-Party Incidents - Open Cases	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Shows all cases involving third-party systems that are still open.
Unsuccessful Administrative Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays all failed logins with an administrative account to assets categorized as Third Party.

Resource	Type	URI	Description
Unsuccessful User Logins from Third Party Systems	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	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/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Displays all failed logins with a non-administrative account to assets categorized as Third Party.
Attack from Third-Party System	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 15 Supplier relationships/15.2 Supplier service delivery management/15.2.1 Monitoring and review of supplier services/	Selects attacks from third-party systems.

ISO 16: Information Security Incident Management Resources

Resource	Type	URI	Description
All Attacks and Suspicious Activity Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all attack and suspicious activity events.
Attacks and Suspicious Activity Targeting Public Facing Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all events where the target asset or zone is categorized in the Public-Facing asset category.

Resource	Type	URI	Description
Attacks and Suspicious Activity Targeting Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all attack and suspicious activity events where the target is an asset from Third Party asset category.
Attacks and Suspicious Activity from Public Facing Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all attack and suspicious activity events where the source asset or zone is categorized in the Public-Facing asset category.
Attacks and Suspicious Activity from Third Party Resources	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all attack and suspicious activity events where the attacker is an asset from Third Party asset category.
High Priority Events	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows high priority events which translate into high risk.
Internal Reconnaissance	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows reconnaissance events originating internal to the corporation.

Resource	Type	URI	Description
Attacks and Suspicious Activity	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays information about attacks and suspicious activity events.
Internal Reconnaissance	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays information about internal reconnaissance events and sources.
Risk - Geo View	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Provides a geographical view of potential threatening events.
Risk Overview	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays high-level information around potential malicious events.
All Attacks - GeoView	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all the attack events on a map.

Resource	Type	URI	Description
Attacks and Suspicious Activity Event Names - Event Graph	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	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	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows connection between source and destination machines and ports as they appear in attack and suspicious activity events.
Attacks per Asset Category	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the number of attacks targeting each of the network domains.
Compromised Hosts	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This Last State data monitor shows the last compromised hosts.
Internal Reconnaissance	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This Event Graph data monitor shows all internal reconnaissance activity.

Resource	Type	URI	Description
Last 10 High Risk Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays in real-time the last 10 Internal Reconnaissance Events.
Last 10 Internal Reconnaissance Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays in real-time the last 10 Internal Reconnaissance Events.
Last 20 Attacks and Suspicious Activity Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays the last 20 attack and suspicious activity events.
Ports Used in Attacks and Suspicious Activity Events	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the ports used in attack and suspicious activity events. By default the data monitor shows data from the last 5 minutes.
Priority Distribution	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the distribution of priorities across all events.

Resource	Type	URI	Description
Reconnaissance Only - GeoView	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows all reconnaissance events on a world map.
Top Internal Reconnaissance Sources	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top internal reconnaissance sources identified by the rule in this section.
Top Internal Reconnaissance Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top internal reconnaissance targets identified by the rule in this section.
Attacks and Suspicious Activity	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Identifies events which indicate compromise, reconnaissance, hostile, or suspicious activity.
Attacks with Geo Information	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Selects attack events with populated Geo fields for both the attacker and target addresses.

Resource	Type	URI	Description
Compromises	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Identifies generic compromises.
High Priority Events	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This filter shows events in which the Priority field is 10.
Information Security Incidents	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Identifies various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.
Internal Recon	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Identifies reconnaissance events that originated internal to the organization. This could indicate that someone is trying to scan the network which is a policy violation.
Reconnaissance - Geo Information	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Identifies reconnaissance events in which the Geo information fields are populated for both attacker and target.

Resource	Type	URI	Description
IT Governance Case Created	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Identifies events where a new case is created.
Attacks and Suspicious Activities	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Provides a listing of all hostile or suspicious events sorted by the event's end time.
Attacks and Suspicious Activities Trend	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This query summarizes the number of attacks and suspicious activities for long term reporting.
Count of Attacks and Suspicious Activities Per Attacker Machine	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	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/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Provides a count of target addresses appearing in of hostile or suspicious events.

Resource	Type	URI	Description
Count of Attacks and Suspicious Activity Event Names	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This report counts the names of attack and suspicious activity events.
Count of Attacks and Suspicious Activity Event Names on Network Domains	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This report counts the names of attack and suspicious activity events on a particular Network Domain.
Count of Attacks and Suspicious Activity Per Day	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This query counts the total number of weekly attack and suspicious activity events.
High Priority Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows events in which the Priority is 10.
Internal Reconnaissance Events	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top events executed for internal reconnaissance.

Resource	Type	URI	Description
Internal Reconnaissance Sources	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top sources conducting internal reconnaissance.
Internal Reconnaissance Targets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top targets accessed by internal reconnaissance activity.
Trend of Attacks and Suspicious Activities By Attacker Address	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Provides a weekly count of attacker addresses appearing in hostile or suspicious events.
Trend of Attacks and Suspicious Activities By Target Address	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Provides a weekly count of target addresses appearing in hostile or suspicious events.
Average Time to Resolution - By Case Severity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.

Resource	Type	URI	Description
Average Time to Resolution - By Day	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	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/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	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/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	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/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Provides a breakdown by owner of all cases.
Cases by Stage	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Provides an overview of all cases in their current stages.

Resource	Type	URI	Description
ISO 5 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 5 section rules actions.
ISO 6 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 6 section rules actions.
ISO 7 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 7 section rules actions.
ISO 8 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 8 section rules actions.
ISO 9 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 9 section rules actions.

Resource	Type	URI	Description
ISO 10 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 10 section rules actions.
ISO 11 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 11 section rules actions.
ISO 12 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 12 section rules actions.
ISO 13 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 13 section rules actions.
ISO 14 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 14 section rules actions.

Resource	Type	URI	Description
ISO 15 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 15 section rules actions.
ISO 16 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 16 section rules actions.
ISO 17 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 17 section rules actions.
ISO 18 Case Overview	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 18 section rules actions.
Open Cases	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows all currently open cases.

Resource	Type	URI	Description
Open Cases by ISO Section	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows all currently open cases by ISO sections.
Open Cases by ISO Section and Severity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows a breakdown of open cases by severity for each regulation section.
Open Cases by Severity	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases by severity.
ISO 5 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 5 rule actions.
ISO 6 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 6 rule actions.

Resource	Type	URI	Description
ISO 7 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 7 rule actions.
ISO 8 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 8 rule actions.
ISO 9 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 9 rule actions.
ISO 10 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 10 rule actions.
ISO 11 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 11 rule actions.

Resource	Type	URI	Description
ISO 12 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 12 rule actions.
ISO 13 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 13 rule actions.
ISO 14 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 14 rule actions.
ISO 15 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 15 rule actions.
ISO 16 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 16 rule actions.

Resource	Type	URI	Description
ISO 17 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 17 rule actions.
ISO 18 Case Overview	Query Viewer	/All Query Viewers/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows the number of open cases per stage for cases that have been created as a result of ISO 18 rule actions.
Attacks and Suspicious Activities	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays a count of the event names of attack and suspicious activity events in a particular Network Domain sorted by the most common events. It also displays the number of unique target machines that were affected by the event. The Network Domain of interest should be specified at report runtime (default: Development Network Domain).
Attacks and Suspicious Activity Weekly Trend	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays a weekly overview of attack and suspicious activity events.
Count of Attacks and Suspicious Activities per Attacker Machine	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This reports shows a count of attack and suspicious activity events per attacker machine.

Resource	Type	URI	Description
Count of Attacks and Suspicious Activities per Target Machine	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This reports shows a count of attack and suspicious activity events per target machine.
Count of Attacks and Suspicious Activity Event Names	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays a count of the event names of attack and suspicious activity events sorted by the most common events. It also displays the number of unique target machines that were affected by the event.
Count of Attacks and Suspicious Activity Event Names in the Network Domain	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Displays a count of the event names of attack and suspicious activity events in a particular Network Domain sorted by the most common events. It also displays the number of unique target machines that were affected by the event. The Network Domain of interest should be specified at report runtime (default: Development Network Domain).
High Priority Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows events in which the Priority field is 10.
Internal Reconnaissance Sources	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top sources conducting internal reconnaissance.

Resource	Type	URI	Description
Internal Reconnaissance Top Events	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top events executed for internal reconnaissance.
Internal Reconnaissance Top Targets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	Shows the top targets accessed by internal reconnaissance activity.
Average Time to Resolution - By Case Severity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	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/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	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/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows how long it is taking individuals to close their cases. This report should be run once a week and reported to management.

Resource	Type	URI	Description
Cases by Stage	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	This report provides an overview of all cases and their current stages.
Open Cases by ISO Section	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows all currently open cases by ISO Section.
Open Cases by ISO Section and Severity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows all currently open cases by ISO Section and Severity.
Open Cases by Owner	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	This report provides a breakdown by owner of all open cases.
Open Cases by Severity	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	Shows all currently open cases by severity.

Resource	Type	URI	Description
Information Security Incident	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 16 Information Security Incident Management/16.1.2 Reporting information security events/	Fires for various kinds of information security incidents such as malicious code activities, denial of service attacks and policy violations.
Internal Recon Detected	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 16 Information Security Incident Management/16.1.2 Reporting information security events/	Selects internal reconnaissance activity.
Severely Attacked System	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 16 Information Security Incident Management/16.1.2 Reporting information security events/	Selects an accumulation in attacks targeting a single machine.

Resource	Type	URI	Description
Multiple Cases Created on Short Period	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 16 Information Security Incident Management/16.1.5 Response to information security incidents/	This rule triggers when multiple cases created on short period of time.
Attacks and Suspicious Activities Trend	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.2 Reporting information security events/	This trend stores long term aggregated information about attacks and suspicious activity events.
Case History	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 16 Information security incident management/16.1.5 Response to information security incidents/	This trend stores all case audit events.

ISO 17: Information Security Aspects of Business Continuity Management Resources

Resource	Type	URI	Description
Critical Assets Resource Exhaustion	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows critical systems resource exhaustion.
Critical Systems Startup and Shutdown	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows critical systems startup and shutdown events.

Resource	Type	URI	Description
Information System Failures on Critical Assets	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Selects information system failures on critical assets.
Up Down Status of Highly Critical Assets	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the state of highly critical assets and whether they are up or down.
Last 10 Shutdowns of Highly Critical Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Displays the last 10 Shutdowns of Highly Critical Assets.
Top 10 Shutdowns of Highly Critical Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the 10 highly critical assets with top shutdowns.
Up Down Status of Highly Critical Assets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the state of highly critical assets and whether they are up or down.
Information System Failures	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Identifies information system failures.
Startup and Shutdown of Highly Critical Assets	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Identifies startups and shutdowns of highly critical machines.
System Shutdown	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Identifies system shut downs.

Resource	Type	URI	Description
System Shutdown of Highly Critical Assets	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Identifies system shut downs of highly critical assets.
System Startup	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Identifies system startups.
Resource Exhaustion Detected on Critical Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the resources reaching their upper end of utilization (for capacity management and planning purposes) on critical assets.
Fault Logs on Critical Machines	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	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/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the critical information system which generated error log entries.
Shutdown of Critical Machines	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows all shutdown events of machines categorized as critical or highly critical.
Weekly Trend - Shutdown of Critical Machines per Day	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	This query is based on trend "Shutdown of Critical Machines" and shows all weekly shutdown events of machines which are categorized as critical.
Weekly Trend -Top 10 Shutdowns of Highly Critical Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	This query is based on trend "Shutdown of Critical Machines" and shows top 10 shutdowns of critical assets on the last week.

Resource	Type	URI	Description
Fault Logs on Critical Machines	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	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/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows the critical information system which generated error log entries.
Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows all shutdown events of machines categorized as critical on the last day.
Weekly Trend - Shutdown of Critical Machines	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Shows a weekly trend of critical machines shutdown.
Information System Failures of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 17 Information Security Aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Selects information system failure events from highly critical machines.
Resource Exhaustion of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 17 Information Security Aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Selects Resource Exhaustion events from highly critical machines.
Shutdown of Highly Critical Machine	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 17 Information Security Aspects of business continuity management/17.1 Information security continuity/17.1.3 Verify, review and evaluate information security continuity/	Selects shutdown events from highly critical machines.
Shutdown of Critical Machines	Trend	/All Trends/ArcSight Solutions/IT Governance/ISO 17 Information security aspects of business continuity management/17.1.3 Verify, review and evaluate information security continuity/	Stores long term aggregated information about shutdown of critical machines.

ISO 18: Compliance Resources

Resource	Type	URI	Description
Intellectual Property Rights Violations	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Selects intellectual property rights violations. To do so, it shows all the rule-firings that are indicating intellectual property rights violations.
Organizational Records Information Leaks	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Shows real-time feed of events reflecting organizational information leakage.
Personal Information Leak	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.4 Privacy and protection of personally identifiable information/	Shows real-time feed of events reflecting personal information leakage.
Technical Compliance Check Failures	Active Channel	/All Active Channels/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Selects events which indicate that a technical compliance check failed, meaning that an either misconfigured system or system with severe vulnerability was found.
Intellectual Property Rights Violations	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Displays information around violations and violators of IPR.
Organizational Information Leak	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Displays information around organizational information leakage.
Personal Information Leak	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.4 Privacy and protection of personally identifiable information/	Displays information around personal information leakage.
Technical Compliance Checking	Dashboard	/All Dashboards/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Displays different views of failed compliance checks.

Resource	Type	URI	Description
Top 10 Intellectual Property Rights Violations	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the top 10 violations concerning intellectual property by looking for the rule-firing in this use-case.
Top 10 Intellectual Property Rights Violators	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the top 10 violators downloading intellectual property by looking for the rule-firing in this use-case.
Last 10 Organizational Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Provides a list of the last 10 information leaks of organizational records.
Top 10 Organizational Records Leak Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Shows the top ten organizational information leak targets.
Last 10 Personal Records Leak	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.4 Privacy and protection of personally identifiable information/	Provides a list of the last 10 information leaks of personal records.
Top 10 Personal Records Leak Targets	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.4 Privacy and protection of personally identifiable information/	Shows the top ten personal information leak targets.
Last 20 Failed Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Shows the last 10 events indicating failed technical compliance checks.
Last 20 Machines Failing Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	This data monitor reports the last 20 machines that were reported to have failed technical compliance check.
Top 10 Failed Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Shows the top ten events indicating failed technical compliance checks.

Resource	Type	URI	Description
Top 10 Machines Failing Technical Compliance Checks	Data Monitor	/All Data Monitors/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Shows the top 10 machines with failed compliance checks.
Intellectual Property Rights Violations	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Identifies violations of intellectual property rights by looking at the rule for this use-case.
Assets with High Severity Vulnerability by Non-Scanners	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	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/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Selects events that indicate the existence of severe vulnerabilities reported by scanners.
Failed Technical Compliance Check	Filter	/All Filters/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Identifies events which indicate a compliance check failure.
Email Policy Violations	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Email.
Policy Violations on Commerce Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Commerce.
Policy Violations on Financial Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Financial.
Policy Violations on HR Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Human Resources.

Resource	Type	URI	Description
Policy Violations on Legal Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Legal.
Policy Violations on PII Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Electronic PII (Personally identifiable information).
Policy Violations on Production Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Production.
Policy Violations on Public Facing Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Public Facing.
Policy Violations on Third-Party Assets	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Third-Party.
Remote Access Policy Violations	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Remote Access.
Wireless Policy Violations	Focused Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.2 Compliance with security policies and standards/	Provides a listing of events categorized by ArcSight as policy violations targeting assets categorized as Wireless.
Intellectual Property Rights Violations	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the various intellectual property rights violations.

Resource	Type	URI	Description
Intellectual Property Rights Violations from Third-Party Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the various third party intellectual property rights violations.
Intellectual Property Rights Violators	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows all the assets which violated intellectual property rights.
Intellectual Property Rights Violators from Third Party-Assets	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows all the third party assets which violated intellectual property rights.
Organizational Records Information Leaks Originated from Third Party	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Shows communications which were classified as information leaks of organizational records originated from third-party assets.
Assets that Failed Technical Compliance Check	Query	/All Queries/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	This query finds assets which failed the technical compliance check.
Intellectual Property Rights Violations	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the different intellectual property rights violations.
Intellectual Property Rights Violations from Third-Party	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows the different intellectual property rights violations.
Intellectual Property Rights Violators	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows all the assets which violated intellectual property rights.

Resource	Type	URI	Description
Intellectual Property Rights Violators from Third-Party	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Shows all the assets which violated intellectual property rights.
Organizational Records Information Leaks on Financial Assets	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Shows the communications which were classified as information leaks of financial organizational records
Assets that Failed Technical Compliance Check	Report	/All Reports/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.2 Information security reviews/18.2.3 Technical compliance review/	Shows assets which failed the technical compliance check.
Intellectual Property Rights Violation	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.2 Intellectual property rights/	Selects intellectual property rights violations. The filter references should be configured to contain all the events pertaining to this use-case. The filter is located in the My Filters group.
Organizational Data Information Leak	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.3 Protection of records/	Selects any organizational information being sent out of the corporate network.
Personal Information Leak	Rule	/All Rules/ArcSight Solutions/IT Governance/ISO 18 Compliance/18.1 Compliance with legal and contractual requirements/18.1.4 Privacy and protection of personally identifiable information/	Selects any personal information being sent out of the corporate network.

Appendix 4: Compare, Backup, and Uninstall Packages

This chapter provides instructions to allow you to generate a list of resource changes, back up the solution package or uninstall the Solution for ITGov CIP 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.

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 Solution for ITGov CIP, navigate to `ArcSight Solutions/IT Governance 5.0`.
3. Right-click the solution package ( ) and select **Compare Archive with Current Package Contents**.

   In the Viewer panel, 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 this table 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 Solution for ITGov CIP, navigate to `ArcSight Solutions/IT Governance 5.0`.
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 to 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 Solution Package

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

For example, if the Solution for ITGov CIP and the PCI solution are both installed on the same ArcSight 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 Solution for ITGov CIP into a different package bundle (ARB) file before uninstalling 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 uninstallation. For detailed instructions, see "Generate a List of Resource Changes" on the previous page.

To uninstall the solution package:

1. Log into the ESM Console as a user with administrative privileges.
2. Click the Packages tab in the Navigator panel.
3. In the Packages tab of the Navigator panel, navigate to `ArcSightSolutions/IT Governance 5.0`.
4. Right-click the `IT Governance 5.0` 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 IT Gov 5.0)

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!