
Micro Focus Security ArcSight ESM

Software Version: 7.6.4

ArcSight Administration and ArcSight System Standard Content Guide



Legal Notices

Copyright Notice

© Copyright 2001-2023 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

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://www.microfocus.com/documentation/arcSight/

Contents

- Chapter 1: What is Standard Content? 9

- Chapter 2: Installation and Configuration 15
 - Modeling the Network 15
 - Categorizing Assets 16
 - Configuring Active Lists 16
 - Configuring Filters 17
 - Enabling Rules 17
 - Configuring Notifications and Cases 18
 - Configuring Notification Destinations 18
 - Rules with Notifications to the CERT Team 19
 - Rules with Notifications to SOC Operators 19
 - Rules with Notifications to the Device Administrators Group 19
 - Scheduling Reports 20
 - Configuring Trends 20
 - Viewing Use Cases 21

- Chapter 3: ArcSight Administration Content 23
 - Connector Overview 25
 - Configuring the Connector Overview Use Case 25
 - Using the Connector Overview Use Case 25
 - Viewing the Dashboards 25
 - ESM Overview 28
 - Using the ESM Overview Use Case 28
 - Viewing the Dashboard 28
 - Viewing the Active Channel 30
 - Logger Overview 31
 - Configuring the Logger Overview Use Case 31
 - Using the Logger Overview Use Case 32
 - Viewing the Dashboards 32
 - Connector Configuration Changes 34
 - Using the Connector Configuration Changes Use Case 34
 - Viewing the Active Channel 34
 - Running Reports 34

Connector Connection and Cache Status	36
Configuring the Connector Connection and Cache Status Use Case	36
Using the Connector Connection and Cache Status Use Case	37
Viewing the Dashboard	37
Viewing the Active Channels	37
Running Reports	38
ArcSight ESM Device Monitoring	39
Understanding Connector Device Status Events	39
Configuring the ArcSight ESM Device Monitoring Use Case	40
Using the ArcSight ESM Device Monitoring Use Case	41
Viewing the Active Channel	42
Viewing the Dashboards	42
Running Reports	45
ESM Licensing	47
Using the ESM Licensing Use Case	47
ESM User Sessions	49
Using the ESM User Sessions Use Case	49
Viewing the Dashboards	49
Running Reports	49
Actor Configuration Changes	51
Using the Actor Configuration Changes Use Case	51
Viewing the Dashboards	51
Viewing the Active Channel	51
Running Reports	51
ESM Resource Configuration Changes	53
Using the ESM Resource Configuration Changes Use Case	53
Viewing the Dashboard	53
Running Reports	53
Content Management	55
Configuring the Content Management Use Case	55
Using the Content Management Use Case	55
Viewing the Dashboard	56
Running Reports	56
Transformation Hub Monitoring	57
Transformation Hub Monitoring Audit Events	57
Using the Transformation Hub Monitoring Use Case	58
Viewing the Dashboard	58

Viewing the Active Channel	59
Active Passive High Availability Monitoring	60
APHA Monitoring Audit Events	60
Configuring the APHA Monitoring Use Case	61
Using the APHA Monitoring Use Case	61
Viewing the Active Channel	62
Viewing the Dashboard	62
Running the Report	65
ESM Events	66
Using the ESM Events Use Case	66
Viewing the Dashboards	66
Viewing the Active Channels	66
Running Reports	67
ESM Reporting Resource Monitoring	69
Using the ESM Reporting Resource Monitoring Use Case	69
Viewing the Dashboards	69
Viewing the Active Channels	69
Running Reports	70
ESM Resource Monitoring	71
Configuring the ESM Resource Monitoring Use Case	71
Using the ESM Resource Monitoring Use Case	71
Viewing the Dashboards	71
Running Reports	72
ESM Storage Monitoring (CORR-Engine)	75
Using the ESM Storage Monitoring (CORR-Engine) Use Case	75
Viewing the Dashboards	75
Running Reports	75
Logger Events	77
Using the Logger Events Use Case	77
Viewing the Active Channels	77
Logger System Health	78
Configuring the Logger System Health Use Case	78
Using the Logger System Health Use Case	79
Viewing the Dashboards	80
Viewing the Active Channel	80
Chapter 4: ArcSight Foundation Content	81

Security Threat Monitoring	82
Resource Locations:	82
Configuring the Security Threat Monitoring Use Case	83
Configuring the Child Use Cases	83
Using the Security Threat Monitoring Use Case	85
Viewing the Dashboard	86
Threat Intelligence Platform	87
Resource Locations:	87
Configuring the Threat Intelligence Platform Use Case	88
Using the Threat Intelligence Platform Use Case	88
Viewing the Dashboards	89
MITRE ATT&CK Overview Use Case	89
Resources	89
ArcSight ESM SOAR Integration	91
Chapter 5: ArcSight System Content	92
Actor Support Resources	93
Using the Actor Support Resources	93
Priority Formula Resources	94
Configuring the Priority Formula Resources Group	94
Priority Formula Rules	94
System Resources	96
Configuring System Resources	96
Using the System Resources	97
Viewing the Active Channels	97
Reports	98
Integration Commands	98
Appendices	100
ArcSight Administration Content	100
Active Channels	101
Active Lists	101
Dashboards	104
Data Monitors	106
Field Sets	110
Fields	110
Filters	111

Integration Commands, Configuration, and Target	116
Queries	117
Query Viewers	121
Rules	124
Session Lists	129
Use Cases	130
Security Monitoring - Base - Active Lists Content	131
Rules	131
Active Lists	131
Security Monitoring - Base Content	133
Active Channel	133
Active Lists	134
Dashboards	135
Data Monitors	135
Field Set	136
Fields	136
Filters	139
Integration Command and Configuration	140
Queries	140
Query Viewers	141
Report	141
Use Case	141
Security Threat Monitoring Content	141
Active Channels	142
Active Lists	142
Dashboards	143
Data Monitors	144
Fields	145
Field Sets	146
Filters	147
Queries	150
Query Viewers	150
Rules	151
Use Cases	182
Threat Intelligence Platform Content	184
Active Channel	184
Active Lists	184
Dashboards	188

Data Monitor	189
Field Set	189
Fields	189
Filters	208
Integration Commands	211
Queries	212
Query Viewers	215
Rules	218
Trends	227
Use Case	227
Publication Status	228
Send Documentation Feedback	229

Chapter 1: What is Standard Content?

Standard content is a series of coordinated resources, such as dashboards, active channels, reports, filters, rules, and so on that is designed to give you pre-installed comprehensive correlation, monitoring, reporting, alerting, and case management with minimal configuration. The standard content provides a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages (.arb files), some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options.

ArcSight Administration content contains several packages that provide statistics about the health and performance of ArcSight products:

- The ArcSight Administration content package is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
- The ArcSight Admin DB CORR content package is installed automatically with the ArcSight Manager for the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.



Note: The ArcSight Admin DB CORR content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- The ArcSight Content Management content package is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.
- The Transformation Hub Monitoring content package is an optional package that lets you monitor activities with Transformation Hub. If ESM is configured to consume events from Transformation Hub, you can install and use this package during ArcSight Manager installation or from the ArcSight Console any time after installation.
- The ArcSight ESM APHA Monitoring content package is an optional package that lets you monitor systems that use the ESM Active Passive High Availability Module. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- The ArcSight Search Filters content package is installed automatically with the ArcSight Manager. It is used to filter searches performed in the ArcSight Command Center. Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in /All Packages/ArcSight Administration/ArcSight Search Filters are imported but require installation before you can use them.

ArcSight System content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for ready-to-use functionality. The ArcSight Networks package contains zones, and local and global network resources. Zones are provided for IPv4 and IPv6 addresses.



Note: ArcSight System resources manage core functionality. The resources are **locked** to protect them from unintended change or deletion.

ArcSight Foundation content contains the **Shared Libraries**, which are common resources that provide core functionality for common security scenarios:

- Conditional Variable Filters is a library of filters used by variables in standard content report queries, filters, and rule definitions.
- Global Variables contain a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats.
- Network filters contain a set of filters required by ArcSight Administration.

The following resources are packages that you install with the Manager.



Note: The ArcSight Foundation content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- The ArcSight ClusterView is for ESM with distributed correlation. This resource group contains all the resources required to monitor the health of ESM distributed correlation cluster(s). The Cluster View dashboard is available on the ArcSight Command Center. This dashboard provides a visual map of your cluster configuration, EPS, available node services, connections, and cluster audit events. The ArcSight Console provides a ClusterView icon that changes color if something is wrong with connections. Users can click on the icon from the Console, which launches the Command Center dashboard. This ClusterView icon on the Console is disabled if you have ESM compact mode.

On the Console, the ClusterView package is located at /All Packages/ArcSight Foundation/ArcSight ClusterView. However, the resources will not be functional in compact mode.

- The ArcSight SocView resource group contains all the resources that provide updated information to the security analysts working for the enterprise's Security Operations Center. Various data monitors displaying information such as Top Attacks, Malicious Activity, destination and source addresses, and so on, are assembled on the SOC Manager dashboard, which is available on the ArcSight Command Center.

On the Console, the package is located at /All Packages/ArcSight Foundation/ArcSight SocView.

- The [Threat Intelligence Platform](#) package contains resources that detect security attacks based on a threat intelligence data feed. This package uses Malware Information Sharing Platform (MISP) as a threat intelligence data feed. The threat intelligence data feed from MISP is directly imported to the ESM using the Model Import Connector (MIC). This package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases. The Threat Intelligence Platform package is an optional package. You have the option to select this optional package for installation while installing the ESM. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version to the current version, you do not have the option to install the Threat Intelligence Platform package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.



Note: This package, along with the Security Threat Monitoring package, feeds data to the MITRE Dashboard. You do not have to install both packages. The MITRE Dashboard works with either individual package (or both). You must install at least one of the packages, however, to use the MITRE Dashboard in the Command Center. Installing this package also installs the Security Monitoring - Base - Active Lists and Security Monitoring - Base packages.

On the Console, the package is located at /All Packages/ArcSight Foundation/Threat Intelligence Platform.

- The [Security Threat Monitoring](#) package monitors security threats based on security log events from the firewall, IDS/IPS, OS, Application, Scanner, Anti-Virus etc. This package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases. The Security Threat Monitoring package is an optional package. While installing the ESM, you have the option to select this package for installation. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version to the current version, you do not have the option to install the Security Threat Monitoring package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.



Note: This package, along with the Threat Intelligence Platform package, feeds data to the MITRE Dashboard. You do not have to install both packages. The MITRE Dashboard works with either individual package (or both). You must install at least one of the packages, however, to use the MITRE Dashboard in the Command Center. Installing this package also installs the Security Monitoring - Base - Active Lists and Security Monitoring - Base packages.

On the Console, the package is located at /All Packages/ArcSight Foundation/Security Threat Monitoring.

- The Security Monitoring - Base package contains shared resources required by the Security Threat Monitoring and Threat Intelligence Platform packages. It also contains content to support the MITRE Dashboard. This base package acts as a supporting package for the Security Threat Monitoring and Threat Intelligence Platform packages. It is mandatory to install this package if you want to use the Security Threat Monitoring and Threat Intelligence Platform packages. This package is automatically installed when you install either both or any one of the Security Threat Monitoring and Threat Intelligence Platform packages. . You can see a full list of resources here.

On the Console, the package is located at /All Packages/ArcSight Foundation/Security Monitoring - Base.

- The Security Monitoring - Base - Active Lists package contains pre-defined active lists required by the Security Monitoring - Base package. This package is a base package which acts as a supporting package for the Security Monitoring - Base package. It is mandatory to install this package if you want to use the Security Threat Monitoring and Threat Intelligence Platform packages. This package is automatically installed when you install either both or any one of the Security Threat Monitoring and Threat Intelligence Platform packages. You can see a full list of resources here.
- The MITRE ATT&CK Use Case allows you to find, filter and display results of the rules used in the Security Threat Monitoring and Threat Intelligence Platform packages.
- The ArcSight ESM SOAR Integration package allows you to define which alerts should be forwarded to SOAR. This is an optional package. If you do not select this package while installing ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ArcSight Console. You can install the package from the console if you do not select it during installation.

On the Console, the package is located at /All Packages/ArcSight Foundation/ArcSight ESM SOAR Integration.

Downloads Groups contains folders used by the security use cases, which are separate content packages that address specific security needs, such as VPN Monitoring, Suspicious Outbound Traffic Monitoring, Anomalous Traffic Detection, Brute Force Attack, and Reconnaissance, to name a few. These use cases are available from the ArcSight Marketplace portal.

Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in /All Packages/Downloads are imported but require installation.



Caution: The resources in the ArcSight Administration, ArcSight DB CORR, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; Micro Focus recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

This document describes how to configure and use the standard content. For detailed information about using ArcSight ESM, see the ArcSight ESM documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Security Use Case Guides, Release Notes, and individual SmartConnector Guides are available on the [ESM documentation page](#).

For detailed information on the ArcSight ESM standard content resources, see the ArcSight ESM Standard Content Resources document, which is available on the [ESM documentation page](#).

Chapter 2: Installation and Configuration

Standard content is required for basic functionality and is pre-installed on the ArcSight Manager. You do not have to perform any additional installation tasks. However, some basic configuration is recommended to tailor the content for your operating environment.



Note: **ArcSight Content Management**, **ESM APHA Monitoring**, and **Transformation Hub Monitoring** are *optional* packages provided in the ArcSight Administration package group. You can install either of these packages during ESM installation or from the ArcSight Console any time after installation.

To install after installation, go to the **Packages** tab in the Navigator, open the ArcSight Administration group, right-click the package you want to install and select **Install Package**. After you install the package, the ArcSight Administration group on the Use Cases tab lists the content use cases.

For detailed information about installing ESM, refer to the [Installation Guide](#).

The list below shows the general tasks you need to complete to configure content with values specific to your environment.

Modeling the Network

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates some of the standard content and makes it effective.

There are several ways to model your network. For information about populating the network model, refer to the [ArcSight Console User's Guide](#). To learn more about the architecture of the network modeling tools, refer to [ESM 101](#).

Categorizing Assets

After you have populated your network model with assets, apply the standard asset categories to activate standard content that uses these categories.

Asset Category	Description
/Site Asset Categories/ Address Spaces/Protected	<p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as <i>Protected</i>.</p>
/System Asset Categories/ Criticality/High	<p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.</p>
/System Asset Categories/ Criticality/Very High	Same as /System Asset Categories/ Criticality/High

You can assign asset categories to assets, zones, asset groups, or zone groups. If assigned to a group, all resources under that group inherit the categories.

You can assign asset categories individually using the Asset editor or in a batch using the Network Modeling wizard. For information about how to assign asset categories using the ArcSight Console tools, refer to the [ArcSight Console User's Guide](#).

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, refer to the [ArcSight Console User's Guide](#) or [ESM 101](#).

Configuring Active Lists

The standard content includes active lists. Certain active lists are populated automatically during run-time by rules. You do not have to add entries to these active lists manually before you use them. Other active lists are designed to be populated *manually* with data specific to your environment. After the lists are populated with values, they are referenced by active channels, filters, rules, reports, and data monitors to provide more information about the assets in your environment.

You can add entries manually to active lists using the following methods. Both methods are described in the [ArcSight Console User's Guide](#).

- One by one using the Active List editor in the ArcSight Console.
- In a batch by importing values from a CSV file.

For a list of the ArcSight Administration active lists you need to configure manually, refer to the configuration information for each use case presented in "[ArcSight Administration Content](#)" on [page 23](#).

For a list of the ArcSight System active lists you need to configure manually, refer to the configuration information for each resource group presented in "[ArcSight System Content](#)" on [page 92](#)

Configuring Filters

For a list of the ArcSight Administration filters you need to configure, refer to the configuration information for each use case presented in "[ArcSight Administration Content](#)" on [page 23](#).

For a list of the ArcSight System filters you need to configure, refer to the configuration information for each resource group presented in "[ArcSight System Content](#)" on [page 92](#).

Enabling Rules

Rules trigger only if they are deployed in the /All Rules/Real-time Rules group and are enabled.

- By default, all the **ArcSight System** rules are deployed in the /All Rules/Real-time Rules group and are also enabled.
- By default, all the **ArcSight Administration** rules are deployed in the /All Rules/Real-time rules group and all rules, are enabled except for all deployed rules under /Logger/System Health.

You can enable the Logger System Health rules if you have a Logger connected to your system. The Logger System Health rules are described in "[Logger Overview](#)" on [page 31](#).

- By default, the rules in the optional **Content Management** package under ArcSight Administration, are deployed in the Real-time Rules group but are disabled.
- By default, the rules in the optional **ArcSight ESM APHA Monitoring and Transformation Hub Monitoring** packages under ArcSight Administration are deployed in the Real-time Rules group and are also enabled.

To enable or disable a rule:

1. In the Navigator panel, go to **Rules** and navigate to the Real-time Rules group.
2. Navigate to the rule you want to enable or disable.
3. Right-click the rule and select **Enable Rule** to enable the rule or **Disable Rule** to disable the rule.

Configuring Notifications and Cases

Standard content depends on rules to send notifications and open cases when conditions are met. Notifications and cases are how you can track and resolve the security issues that the content is designed to find.

By default, most notifications and create case actions are disabled in the standard content rules that send notifications about security-related events.

To enable rules to send notifications and open cases, first configure notification destinations (see "[Configuring Notification Destinations](#)" below), then enable the notification and case actions in the rules. For more information about working with Rule actions in the Rules Editor, refer to the [ArcSight Console User's Guide](#).

Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, most notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules.

The notification action is enabled by default in the following standard content rules:

- ArcSight Administration/Devices/**Alert - Critical Devices inactive for more than 1 hour**
- ArcSight Administration/ESM/APHA Monitoring/**Alert - APHA Status Change**
- ArcSight Administration/ESM/System Health/Resources/Domains/**Out of Domain Fields**
- ArcSight Administration/ESM/System Health/Storage/**ASM Database Free Space - Critical**

Make sure you configure notification destinations for the Device Administrators, SOC Operators, and the CERT team groups so that the notifications are received.

Refer to the [ArcSight Console User's Guide](#) for information on how to configure notification destinations.

Rules with Notifications to the CERT Team

The following rule is configured to send notifications to the **CERT Team** notification destination group.

Rule Name	Rule URI
Out of Domain Fields	ArcSight Administration/ESM/System Health/Resources/Domains/



Note: The notification action for the **Out of Domain Fields** rule is enabled by default. Make sure you configure destinations for the CERT team to receive notifications when this rule triggers.

Rules with Notifications to SOC Operators

The following rules are configured to send notifications to the **SOC Operators** notification destination group.

Rule Name	Rule URI
Connector Dropping Events	ArcSight Administration/Connectors/System Health/
Connector Still Down	ArcSight Administration/Connectors/System Health/
Connector Still Caching	ArcSight Administration/Connectors/System Health/
Excessive Rule Recursion	ArcSight Administration/ESM/System Health/Resources/Rules/
Rule Matching Too Many Events	ArcSight Administration/ESM/System Health/Resources/Rules/
ASM Database Free - Critical	ArcSight Administration/ESM/System Health/Storage/
Alert - APHA Status Change	ArcSight Administration/ESM/APHA Monitoring



Note: The notification action for the **ASM Database Free Space - Critical** and **Alert - APHA Status Change** rules is enabled by default. Make sure you configure destinations for the SOC Operators group to receive notifications when these rules trigger.

Rules with Notifications to the Device Administrators Group

The following rule is configured to send notifications to the **Device Administrators** notification destination group:

Rule Name	Rule URI
Alert - Critical Devices inactive for more than 1 hour	ArcSight Administration/Devices/



Note: The notification action in this rule is enabled by default. Make sure you configure destinations for the Device Administrators group to receive notifications when this rule triggers. See "[Configuring the ArcSight ESM Device Monitoring Use Case](#)" on page 40.

Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. By default, reports are not scheduled to run automatically.

Evaluate the reports that come with the content, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the [ArcSight Console User's Guide](#).

Configuring Trends

Trends are a type of resource that can gather data over longer periods of time and can then be leveraged for reports. Trends streamline data gathering to the specific pieces of data you want to track over a long range, and breaks the data gathering up into periodic updates. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources. Trends can also provide a snapshot of which devices report on the network over a series of days.

ArcSight System content does not contain any trends. ArcSight Administration content includes trends, which are enabled by default. Majority of these enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually less busy than during peak daytime business hours. Exceptions are two /All

Trends/Arcsight Administration/ESM trends:

- /Licensing/Storage Licensing Data is scheduled to run daily at 10:52.22 a.m.
- /System Health/Storage/ASM Database Free Space is scheduled to run daily at 2:34 p.m.

You can customize these schedules to suit your needs using the Trend scheduler in the ArcSight Console.

To disable a trend, go to the Navigator panel, right-click the trend you want to disable and select **Disable Trend**.



Caution: To enable a disabled trend, you must first **change the default start date** in the Trend editor.

If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and back fills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

For more information about trends, refer to the [ArcSight Console User's Guide](#).

ArcSight Administration contains resources that enable you to monitor the performance of your enabled trends. The **Trend Details** dashboard in the **ESM Reporting Resource Monitoring** use case (described on page 69) shows the runtime status for all enabled trends. The trend reports show statistics about trend performance for all enabled trends.

Viewing Use Cases

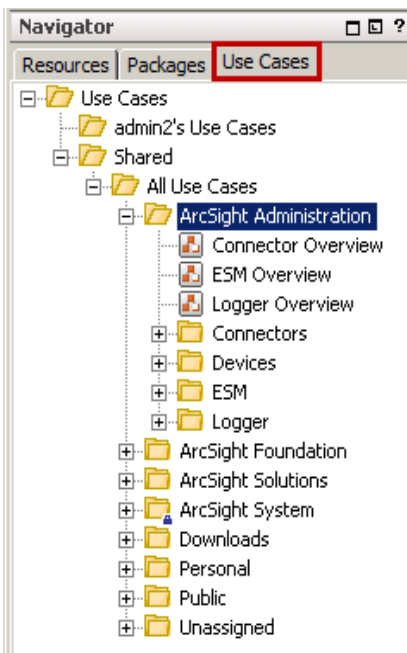
ArcSight Administration resources are grouped together in the ArcSight Console in use cases. A use case groups a set of resources that help address a specific issue or business requirement.



Note: Currently, ArcSight System content does not contain any use cases. "[ArcSight System Content](#)" on page 92 documents System resources by grouping them by function.

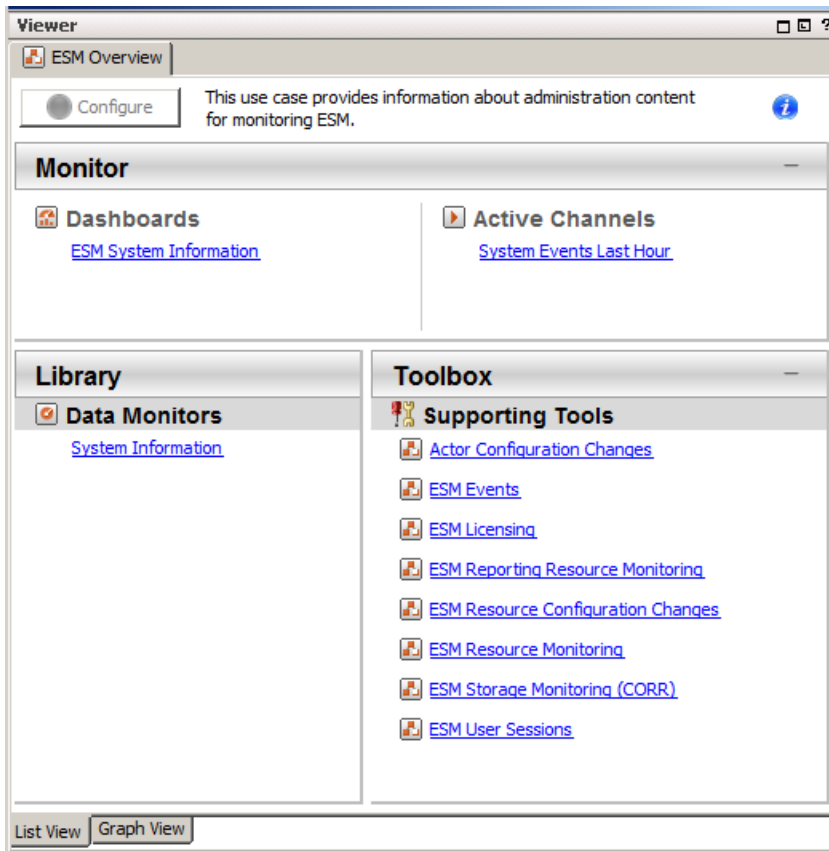
To view the resources in a use case:

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



2. Browse for a use case; for example, ArcSight Administration/ESM Overview.
3. Right-click the use case and select **Open Use Case**, or double-click the use case.

The use case with its associated resources displays in the Viewer panel of the ArcSight Console.



Chapter 3: ArcSight Administration Content

The ArcSight Administration resources provide statistics about the health and performance of the ArcSight system and its components. This content is essential for managing and tuning performance.

The ArcSight Administration use cases are listed in the table below.



Note: ArcSight Administration relies on a series of common resources that provide core functions for common security scenarios. These common resources are located under the Common group. You can identify these resources by the URI; for example, `ArcSight Foundation/Common/Network Filters/`.

Use Case	Purpose
Overview	
"Connector Overview" on page 25	Provides administration content for monitoring connectors and devices.
"ESM Overview" on page 28	Provides administration content for monitoring the system.
"Logger Overview" on page 31	Provides Logger status and statistics.
Connectors	
"Connector Configuration Changes" on page 34	Provides information about configuration changes (such as upgrades) and the versions of the connectors on the system.
"Connector Connection and Cache Status" on page 36	Provides the connection status and caching status of connectors on the system.
Devices	
"ArcSight ESM Device Monitoring" on page 39	Provides resources to help you monitor the status of devices that send events to connectors.
ESM	
"ESM Licensing" on page 47	Provides information about licensing compliance.
"ESM User Sessions" on page 49	Provides information about user access to the system.
ESM - Configuration Changes	
"Actor Configuration Changes" on page 51	Provides information about changes to the actor resources.
"ESM Resource Configuration Changes" on page 53	Provides information about changes to the various resources, such as rules, reports, and so on.
ESM - Content Management	

Use Case	Purpose
"Content Management" on page 55	Provides information about content package synchronization with the Content Management feature, including the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.
ESM - APHA Monitoring	
Active Passive High Availability Monitoring	Provides resources to help you monitor the status of ESM systems that are using the optional ESM Active Passive High Availability Module (APHA Module). The APHA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.
ESM - Transformation Hub Monitoring	
"Transformation Hub Monitoring" on page 57	Provides resources to help you monitor the status of connectivity and event consumption between a Transformation Hub deployment and ESM.
ESM - System Health	
"ESM Events" on page 66	Provides statistics on the flow of events through the system.
"ESM Reporting Resource Monitoring" on page 69	Provides performance statistics for reports, trends, and query viewers.
"ESM Resource Monitoring" on page 71	Provides processing statistics for various resources, such as trends, rules, and so on.
"ESM Storage Monitoring (CORR-Engine)" on page 75	Provides information on the health of the CORR- (Correlation Optimized Retention and Retrieval) Engine.
Logger	
"Logger Events" on page 77	Provides statistics for events sent through a Logger.
"Logger System Health" on page 78	Provides performance statistics for any Logger connected to the system.

Connector Overview

The Connector Overview use case provides resources to help you monitor connectors and devices.

Configuring the Connector Overview Use Case

The Connector Overview use case uses the following active lists from the Connector Connection and Cache Status use case:

- **Connector Information**
- **Connectors - Caching**
- **Connectors - Down**
- **Connectors - Dropping Events**
- **Connectors - Still Caching**
- **Connectors - Still Down**
- **Black List - Connectors**

For information about configuring these active lists, refer to the configuration section in ["Connector Connection and Cache Status" on page 36](#).

Using the Connector Overview Use Case

The **Connector Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

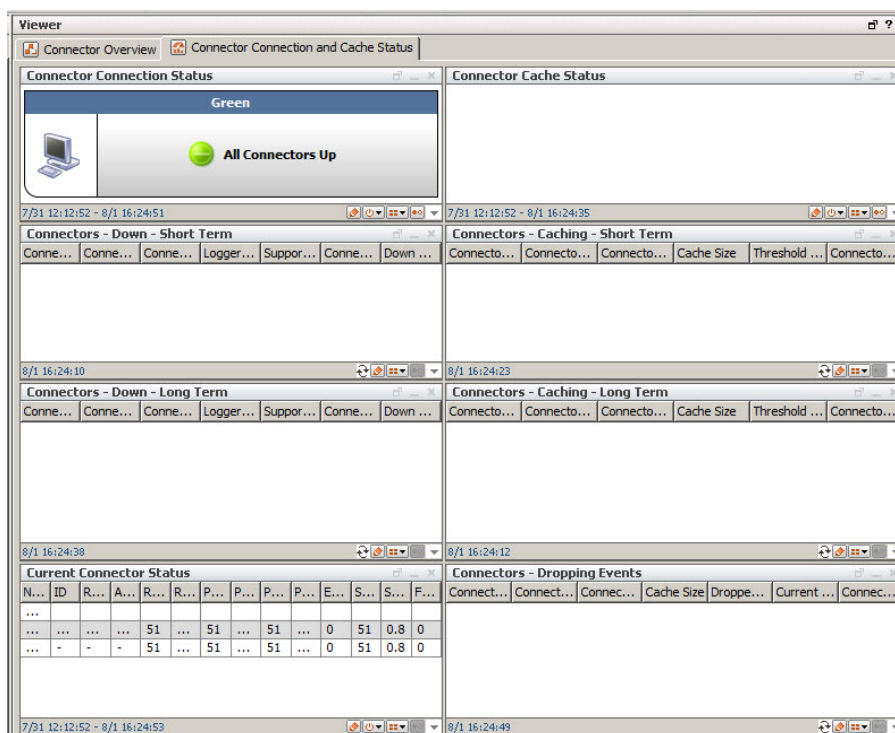
The Monitor section of the use case provides two dashboards to help you monitor the status of your connectors and see the top devices that are contributing events. The Library section of the use case lists supporting resources.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- The **Current Event Sources** dashboard shows the top 20 devices that are contributing events. The device vendor and product type are listed.

- The **Connector Connection and Cache Status** dashboard displays the overall status of connectors and provides information about connectors that are down, caching, or dropping events. An example dashboard is shown below.



Focus on any yellow or red icons, as they represent connectors that might require attention.

The **Connectors - Down - Short Term** and **Connectors - Down - Long Term** query viewers show connectors that have been down for less than 20 minutes (yellow icons) and for more than 20 minutes (red icons). Down time of less than 20 minutes might be acceptable; for example, scheduled maintenance of the host machine on which the connector is installed. However, more than 20 minutes might indicate an issue that requires investigation. Maybe the connector is configured improperly or needs to be restarted; or there is an underlying network, connection, or hardware problem.

You can find more information about each connector in the **Connector Connection Status** and **Connector Cache Status** data monitors. Check the **Failed Connection Attempts** column to see if the connector is repeatedly failing to connect to the ArcSight Manager. (You might need to undock the component to see this column on the far right side.)

The components on the right side of the dashboard show connectors that are caching events instead of sending them to the ArcSight Manager. Short term caching (for less than two hours) is expected behavior when the connector receives bursts of events or when the ArcSight Manager is down. However, investigate long term caching (more than two hours), as it can result in a full cache and the permanent loss of events. Check the **Cache Size** and **Threshold Size** columns to determine if the cache is nearing its maximum capacity. Check

to see if events have been dropped. If so, review the connector logs and ArcSight Manager logs for errors, and adjust the connector configuration properties as needed.

For answers to frequently asked questions about caching, see the *ArcSight SmartConnectors User's Guide*. For configuration information about a specific connector, see the configuration guide for that connector. For information about connector caching issues, check the [Micro Focus Community](#).

ESM Overview

The ESM Overview use case provides resources that help you monitor the ArcSight system. No configuration is required for this use case.

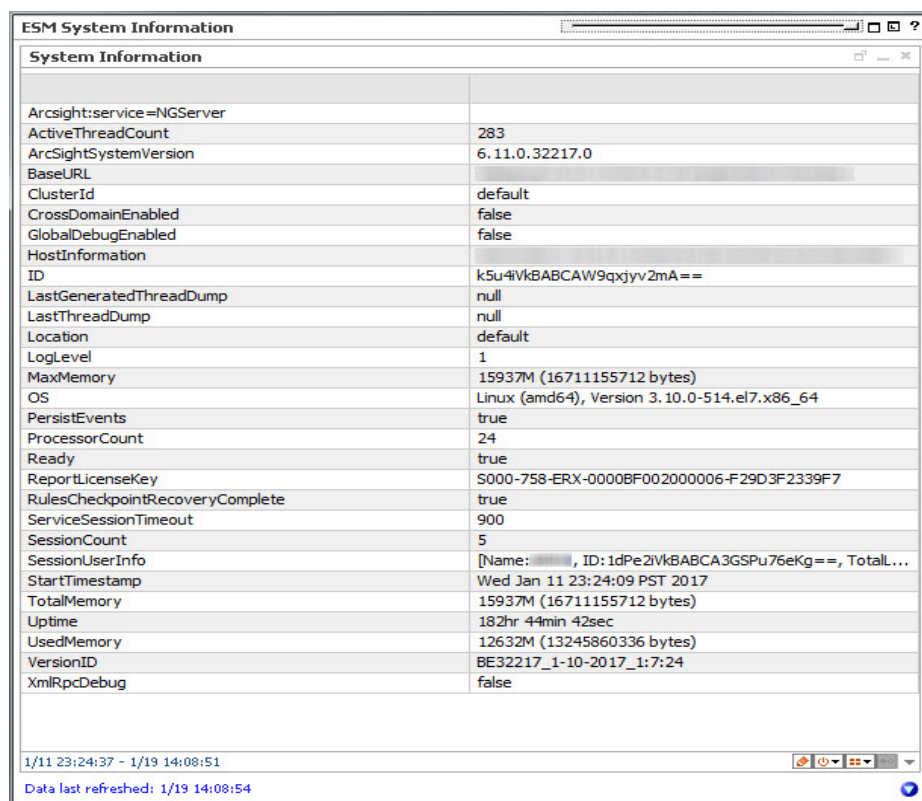
Using the ESM Overview Use Case

The **ESM Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides the **ESM System Information** dashboard to help you monitor your ArcSight system and the **System Events Last Hour** active channel to help you investigate generated events. The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

Viewing the Dashboard

To view the **ESM System Information** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays important information about the ArcSight system, such as the version, license, total amount of memory available to the system, and the amount of used memory. System resource availability and statistics, and other important settings are also shown. Following is an example dashboard:



Some of the information on this dashboard is for internal system use.

System Information Dashboard

System Information	Meaning
Arcsight:service=NGServer	Standard naming convention for the ESM server
ActiveThreadCount	(For internal system use)
ArcSight SystemVersion	ESM release version number, including build number
BaseURL	The URL to the ESM server
ClusterId	(For internal system use)
CrossDomainEnabled	Whether or not the server is enabled for cross-domain requests
GlobalDebugEnabled	(For internal system use)
Host Information	The ESM host name and IP address
ID	Resource ID for the ESM server system as shown in /All Assets/ArcSight System Administration/Managers/<ESM server>
LastGeneratedThreadDump	(For internal system use)
LastThreadDump	(For internal system use)
Location	The physical location of the Manager server, entered during setup (managersetup wizard). Shows default if nothing was entered.

System Information Dashboard, continued

System Information	Meaning
LogLevel	(For internal system use)
MaxMemory	Returns the maximum amount of memory that the Java virtual machine will attempt to use. If there is no inherent limit then the value <code>java.lang.Long.MAX_VALUE</code> will be returned.
OS	Operating system platform on which the ESM server is installed
PersistEvents	Events are persisted on the database
Processor Count	Number of CPU cores on the system
Ready	System is ready
ReportLicenseKey	Unique license key for the ESM Report Template Designer (InetSoft)
RulesCheckpointRecoveryComplete	Denotes the completion of the rules checkpoint process. See the ESM Administrator's Guide for information on the rules checkpoint process.
ServiceSessionTimeout	(For internal system use)
SessionCount	Number of concurrent sessions to ESM using ArcSight Console, ArcSight Command Center, and ESM Web Services.
SessionUserInfo	Login name of the user viewing this dashboard, including the resource ID corresponding to that ESM user.
StartTimeStamp	Date and time when Manager was last started.
TotalMemory	Returns the total amount of memory in the Java virtual machine. The value returned may vary over time, depending on the host environment.
Uptime	Amount of time the system was up and running
UsedMemory	Current Java memory used by ESM
VersionID	ESM build number; concurs with <code>ArcSightSystemVersion</code>
XmlRpcDebug	(For internal system use)

Viewing the Active Channel

To view the **System Events Last Hour** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all events generated by the ArcSight system during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events. Double-click an event to see details about the event in the Event Inspector.

Logger Overview

The Logger Overview use case provides resources to help you monitor Logger status and statistics.

Configuring the Logger Overview Use Case

If you have a Logger connected to your ArcSight system, follow the steps below to configure the Logger Overview use case:

To configure the Logger Overview use case:

1. Enable the following rules in the /All Rules/Real-time Rules/ArcSight Administration/Logger/System Health folder:
 - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
 - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for the same sensor type for a Logger indicate OK.
 - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

For information about enabling rules, refer to ["Enabling Rules" on page 17](#).
2. Edit the **My Logger** filter in the /All Filters/ArcSight Administration/Logger/System Health folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.
3. Enable the following data monitors:
 - a. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview folder:
 - **Logger Disk Usage**
 - **Logger Hardware Status**
 - b. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview

folder:

- **CPU Usage (Percent) - Last 10 Minutes**
- **Disk Read and Write (Kbytes per Second) - Last 10 Minutes**
- **Disk Usage**
- **EPS Usage (Events per Second) - Last 10 Minutes**
- **Memory Usage (Mbytes per Second) - Last 10 Minutes**
- **Network Usage (Bytes) - Last 10 Minutes**
- **Sensor Type Status**



Note: These data monitors are disabled by default to avoid increasing the load on environments without a Logger.

For information about data monitors, refer to the *Enabling or Disabling a Data Monitor* section in the [ArcSight Console User's Guide](#).

Using the Logger Overview Use Case

The **Logger Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor all your ArcSight appliances and the hardware, storage, CPU, memory, network, and EPS usage for a specific Logger. The Library section of the use case lists supporting resources that help compile information in the dashboards.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below:

- **ArcSight Appliances Overview** - Review the data monitors on this dashboard to check your ArcSight appliances. Focus on any red icons, as they represent appliances that might require attention. Examine the disk status for all appliances; a warning or critical status requires your attention.
- **My Logger Overview** - Review the data monitors on the dashboard to check the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the My Logger filter. The information is collected during the last ten minutes.



Note: The data monitors in the **My Logger Overview** and **ArcSight Appliances Overview** dashboards are disabled by default to avoid increasing the load on environments without Logger. Enable these data monitors if you have a Logger in your environment as described in "[Configuring the Logger Overview Use Case](#)" on page 31.

Connector Configuration Changes

The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the connectors on the system. No configuration is required for this use case.

Using the Connector Configuration Changes Use Case

The **Connector Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/Connectors on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides an active channel to help you monitor connector upgrades, and several reports that show the status and historical information about connector upgrades. The Library section of the use case lists supporting resources that help compile information in the active channel and the reports.

Viewing the Active Channel

To view the **Connector Upgrades** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events related to connector upgrades received within the last two hours. The active channel uses the Connector Upgrades field set. Use this active channel as a baseline for your monitoring.

Running Reports

The **Connector Configuration Changes** use case provides several reports that show connector upgrade history. You can provide these historical reports to the stakeholders in your company, when needed.

By default, the reports use data for the last week from the time you run the report. You can change the start and end time of the report for longer- or shorter-term analysis when you run the report.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page

size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- The **Connector Upgrades Count** report shows the total count of successful and failed connector upgrades in a pie chart and the counts per day in a table.
- The **Connector Versions** report lists all the connectors with their latest versions, grouped by connector type, connector zone, and connector address.
- The **Connector Versions by Type** report lists all the connectors by connector type, grouped by connector version, connector zone, and connector address.
- The **Failed Connector Upgrades** report lists the connectors with failed upgrades, grouped by connector zone, connector address, connector name, and connector ID. The report also shows the reason for the failure.
- The **Successful Connector Upgrades** report lists the connectors with successful upgrades, sorted chronologically.
- The **Upgrade History by Connector** report shows the upgrade history by connector sorted chronologically. When running this report, use the connector ID located in the connector resource and copy-paste the ID into the ConnectorID field in the Custom Parameters for the report.
- The **Upgrade History by Connector Type** report shows the upgrade history by connector type, grouped by connector zone, connector address, connector name, and connector ID.
- The **Version History by Connector** report shows the version history by connector, sorted chronologically. When running this report, use the connector ID (located in the connector resource) and copy-paste it in to the ConnectorID field in the Custom Parameters for the report.
- The **Version History by Connector Type** report shows the version history by connector type, grouped by connector zone, connector address, connector name, and connector ID.

Connector Connection and Cache Status

The Connector Connection and Cache Status use case provides the connection status and caching status of connectors on the system. Connectors can be connected directly to the ArcSight system or through Loggers.

Configuring the Connector Connection and Cache Status Use Case

The Connector Configuration and Cache Status use case requires the following configuration for your environment:

Customize the following active lists:

- In the **Connectors - Down** active list, adjust the Time to Live (TTL) attribute, if needed. By default, the TTL is set to 20 minutes. A connector down for fewer than 20 minutes is considered to be down for a short term. After 20 minutes, the entry for this active list expires and the connector information is moved to the **Connectors - Still Down** active list, unless the connector comes back up before 20 minutes.
- In the **Connectors - Caching** active list, adjust the Time to Live (TTL) attribute, if needed. By default, the TTL is set to two hours. A connector that has been caching for fewer than two hours is considered to be caching for a short term. Connectors caching for up to two hours are not considered to be a problem. After two hours, the entry for this active list expires and the connector information is moved to the **Connectors - Still Caching** active list, unless the connector cache is emptied in fewer than two hours, and it is removed by the Connector Cache Empty rule.
- Populate the **Black List - Connectors** active list with the URI and IP address of each connector you want to exclude from being evaluated by the Connector UP and Connector Down rules. These rules detect connectors that are started and are reporting events, and those that are shut down. These rules can send a notification (if notifications are enabled) when the connectors have been down for a certain period of time. You might want to exclude connectors that you start and stop manually, connectors that are scheduled to run once every week (such as vulnerability scanners), or connectors that you are testing (starting and stopping frequently during the setup process).
- *Optional:* Populate the **Connector Information** active list with the contact information for each connector, if needed. For example, you can add contact information for connectors maintained by other individuals or organizations. Add the contact information in the Support Information field in the format provided (poc= | email= | phone= | dept= |

action=).

The Connector Information active list collects information about connectors that have reported into the system, as well as information from the ArcSight Manager when the connector is first registered. Do not add information to this active list for connectors that are not already reported into the system and registered.

For information about how to configure an active list, refer to the [ArcSight Console User's Guide](#).

Using the Connector Connection and Cache Status Use Case

The **Connector Connection and Cache Status** use case is located in /All Use Cases/ArcSight Administration/Connectors on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard, two active channels and two reports to help you monitor connector connection and status. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channels, and reports.

Viewing the Dashboard

To view the **Connector Connection and Cache Status** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the status of your connectors in real time. You can see which connectors have been down for a short time or a long time, and which connectors are dropping or caching events. Use this dashboard as a baseline for your monitoring. Investigate any connectors that have been down for a long period of time and any connectors that are dropping or caching events.

Viewing the Active Channels

The **Connector Connection and Cache Status** use case provides two active channels. To open an active channel in the Viewer panel, click the link for the active channel in the use case.

- The **Connector Caching Events** active channel shows information about connector *cache* status audit events and correlation events from the related connector monitoring rules.
- The **Connector Connection Status Events** active channel shows information about connector *connection* status audit events and correlation events from the related connector monitoring rules.

Running Reports

The **Connector Connection and Cache Status** use case provides two reports that show connector cache history and connector status. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Cache History by Connectors** shows the cache history by connector, sorted chronologically. By default, the report shows all of the connectors known by the system. You can specify the connector URI (located in the Connector Information active list) in the ConnectorURI field in the custom parameters for the report to narrow down the connector cache histories reported, from groups (such as /All Connectors/Site Connectors/) to a specific connector (such as /All Connectors/Site Connectors/DMZ/WUC-1). The default time range of this report is the past three to four months.
- **Current Cache Status** lists the connectors that are currently caching and dropping events.

ArcSight ESM Device Monitoring

The ArcSight ESM Device Monitoring use case enables you to monitor the status of ArcSight ESM devices that send events to SmartConnectors (connectors). You can monitor all devices continuously and detect inactive devices promptly with minimum impact on the ArcSight ESM system. For example, you can see which firewall is inactive, which web server is new, and if a critical device is inactive for more than one hour.

A connector can use the Device Status Monitoring (DSM) feature to generate Connector Device Status events periodically reporting the status of each device communicating with it. A device is a unique combination of these five fields: deviceHostName, deviceVendor, deviceProduct, deviceZone, and customer.

When a device is sending base events to the connector and the connector is receiving them, the status of a device is *active*. When a connector receives no events from a device for a set period of time, the status of a device is *inactive*. The inactive status does not provide details about the network status, hardware or software issues on the device or connector.



Note: The ArcSight ESM Device Monitoring content monitors devices that send events to SmartConnectors (connectors that work on security events). The content does not support Model Import connectors.

Understanding Connector Device Status Events

When DSM is enabled, the connector generates a Connector Device Status internal event for each device it is tracking. The event contains the information in the following table.

To enable DSM, see ["Configuring the ArcSight ESM Device Monitoring Use Case" on the next page](#).

Connector Device Status Event Fields	Field Value
Event Name	Connector Device Status
Device Event Class ID	agent:043
Device Custom String1	device vendor (from the base events received from the device)
Device Custom String2	device product (from the base event received from the device)
Device Custom Number1	total event count (total number of events for this device since the SmartConnector started)

Connector Device Status Event Fields	Field Value
Device Custom Number2	event count SLC (since last check) (number of events for this device since the last internal event was sent)
Source Address	device address (source device sending base events to the connector)
Source Hostname	device hostname (source device sending base events to connector)
Device Custom Date1	Last Event Received (connector time when the last event was received from the device)
deviceEventCategory	/Agent/Connection/Device/Status
agentSeverity	low
deviceVendor	ArcSight
deviceProduct	ArcSight

When a new device sends the first event to the connector, the connector starts generating the Connector Device Status events for this device. The **All Monitored Devices** rule is configured to trigger when the Connector Device Status events have a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check).

Configuring the ArcSight ESM Device Monitoring Use Case

The ArcSight ESM Device Monitoring use case requires the following configuration for your environment:

1. Enable Device Status Monitoring (DSM) on your connector. When DSM is enabled, a Connector Device Status internal event is sent for each device tracked by the connector with the following information: the last time the connector received an event from the device, the total number of events from this device since the connector started, and the number of events sent by this device since the last check.
 - a. On the **Resources** tab of the ArcSight Console Navigator panel, go to **Connectors**, right click the connector on which you want to enable DSM, then select **Configure**.
The **Inspect/Edit** panel for the Connector Editor opens. On the **Connector** tab, the **Name** field is populated automatically with the name assigned during connector installation.
 - b. On the **Default** tab, set the **Enable Device Status Monitoring (in millisec)** option.

By default, DSM is disabled on a connector; the **Enable Device Status Monitoring (in millisec)** option is set to -1. The minimum positive value you can assign is one minute (60000 milliseconds).



Caution: Enabling DSM can create a heavy load on busy connectors. Micro Focus recommends that you set DSM to ten minutes or more; for example, 600000.

- c. Restart the connector.
2. Populate the **Critical Monitored Devices** active list with the devices that are critical in your environment. This active list is then updated automatically when the Critical Monitored Devices rule triggers. The **Critical Monitored Devices** dashboard shows only the devices included in this active list.

To add devices that are critical to your environment, you can export the specific devices from the **All Monitored Devices** active list and import them to the **Critical Monitored Devices** active list. If you have a predefined list of critical devices, you can import a csv file containing all your critical devices to the **Critical Devices** active list. When the Critical Monitored Devices rule triggers, the entries from the **Critical Devices** active list are added to the **Critical Monitored Devices** active list.

3. Populate the **Whitelisted Monitored Devices** active list with the devices that you do not want to monitor. For example, include in this active list non-critical devices or devices that only respond once a day. The **Whitelisted Monitored Devices** active list is used in the **All Monitored Devices** rule condition.
4. Configure notification destinations for the Device Administrators group so that the correct administrators are notified when the **Alert - Critical Devices inactive for more than 1 hour** rule triggers. The send notification action in the **Alert - Critical Devices inactive for more than 1 hour** rule is enabled by default. For details on how to configure notification destinations, refer to the [ArcSight Console User's Guide](#).

Using the ArcSight ESM Device Monitoring Use Case

The **ArcSight Device Monitoring** use case is located in /All Use Cases/ArcSight Administration/Devices on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor your ESM devices, including critical assets, and investigate device status events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.

Viewing the Active Channel

To view the **ArcSight ESM Device Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all Device Status events received within the last two hours. Double-click an event to see details about the event in the Event Inspector.

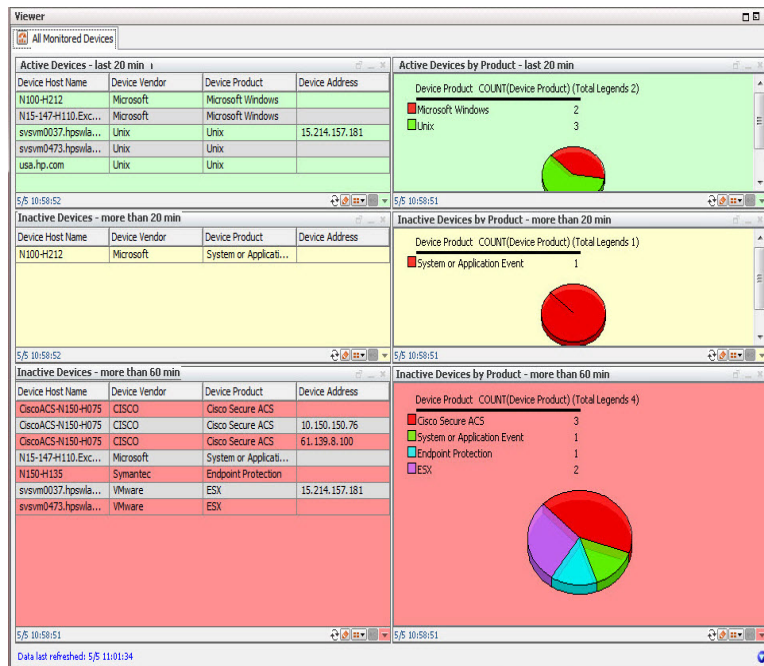
Viewing the Dashboards

The **ArcSight Device Monitoring** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.



Tip: View the dashboards for short-term activity and inactivity monitoring (for example, 20 minutes to one hour). For longer term activity, run the ArcSight ESM Device Monitoring reports. See "[Running Reports](#)" on page 45.

All Monitored Devices Dashboard



This dashboard provides query viewers that show information about all known devices (all the devices in the **All Monitored Devices** active list). The query viewers are color coded so you can identify problems quickly.


- The **Active Devices - last 20 min** query viewer displays information about devices that have reported events within the last 20 minutes. The **Active Devices by Product - last 20**

min query viewer displays the number of devices that have reported events within the last 20 minutes, in a pie chart by device product type.

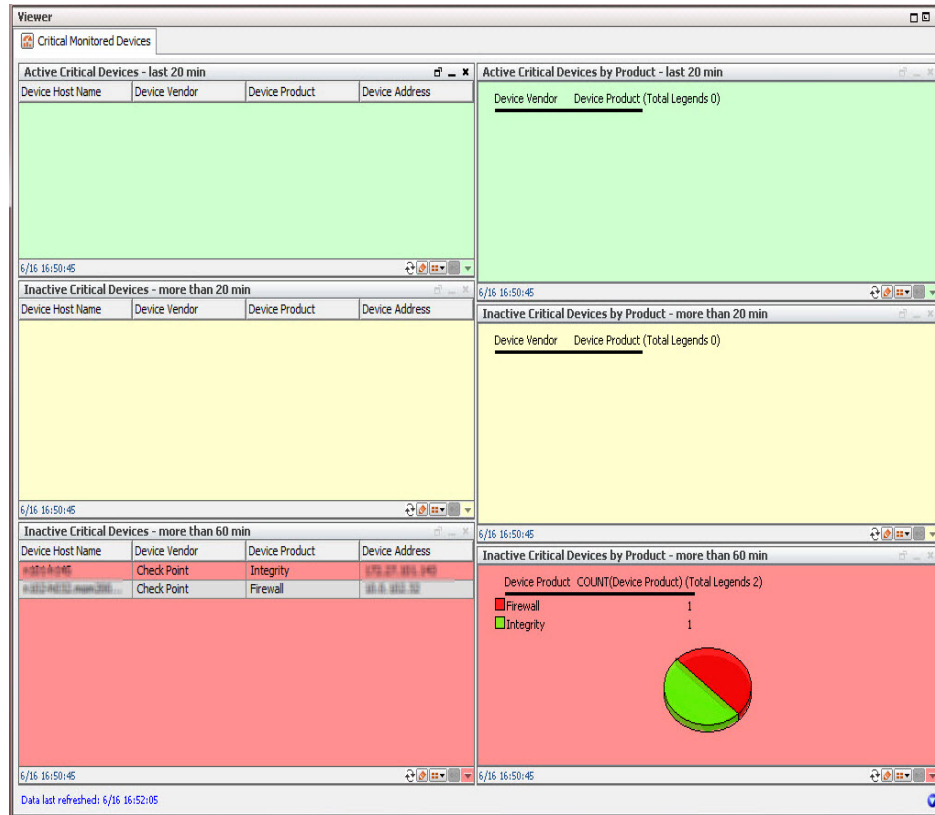
- The **Inactive Devices - more than 20 min** query viewer displays information about devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.
- The **Inactive Devices - more than 60 min** query viewer displays information about devices that have not reported events within the last 60 minutes. The **Inactive Devices by Product - more than 60 min** query viewer displays the number of devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

Focus on the devices in the **Inactive Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

Drill down to see details about an event on the dashboard, such as the Agent Name, Event Count SLC, Creation Time, and so on:

- If the view in the query viewer is a pie chart, change the view to a table (click the **View as** button  on the bottom right of the query viewer).
- Right click an event in the query viewer and select **Drilldown > Show device details for selected Device Product**.

Critical Monitored Devices Dashboard



This dashboard provides several query viewers that show an overview of your critical devices (the devices in the **Critical Monitored Devices** active list).

- The **Active Critical Devices - last 20 min** query viewer displays information about critical devices that have reported events within the last 20 minutes. The **Active Critical Devices by Product - last 20 min** query viewer displays the number of critical devices that have reported events within the last 20 minutes, in a pie chart by device product type.
- The **Inactive Critical Devices - more than 20 min** query viewer displays information about critical devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of critical devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.
- The **Inactive Critical Devices - more than 60 min** query viewer displays information about critical devices that have not reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 60 min** query viewer displays the number of critical devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

Focus on the devices in the **Inactive Critical Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

Running Reports

The **ArcSight Device Monitoring** use case provides several reports that show historical information about your ESM devices. You can provide these historical reports to the stakeholders in your company, when needed. You can run the following reports for longer-term activity and inactivity monitoring.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- The **All Devices Detected Inactive - Last 24 Hours** report displays information about all devices that are *inactive* within the last 24 hours.
- The **All Devices Detected Inactive - Last 7 Days** report displays information about all devices that are *inactive* within the last seven days.
- The **All Monitored Devices** report displays information about all known devices (devices listed in the **All Monitored Devices** active list).
- The **Critical Devices Detected Inactive - Last 24 Hours** report displays information about critical devices that are *inactive* within the last 24 hours (critical devices are listed in the **Critical Monitored Devices** active list).
- The **Critical Devices Detected Inactive - Last 7 Days** report displays information about critical devices that are *inactive* within the last seven days.
- The **Critical Monitored Devices** report displays information about all critical devices being monitored.
- The **New Devices Detected - Last 24 Hours** report displays information about the new devices detected within the last 24 hours.

- The **New Devices Detected - Last 7 Days** report displays information about new devices detected within the last seven days.

ESM Licensing

The ESM Licensing use case provides information about licensing compliance. No configuration is required for this use case.

Using the ESM Licensing Use Case

The **ESM Licensing** use case is located in /All Use Cases/ArcSight Administration/ESM on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several reports that provide a historical view of ESM license compliance. You can provide these reports to the stakeholders in your company, when needed. The Library section of the use case lists supporting resources that help compile information in the reports.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actors Licensing Report** shows the licensing history for actors within the last seven days. A chart shows the current count and the count limit.
- **Assets Licensing Report** shows the licensing history for assets within the last seven days. A chart shows the current count and the count limit.
- **Console Users Licensing Report** shows the licensing history for console users within the last seven days. A chart shows the current count and the count limit.
- **Devices Licensing Report** shows the licensing history for devices within the last seven days. A chart shows the current count and the count limit.
- **Web Users Licensing Report** shows the licensing history for web users (using the ArcSight ESM Command Center) within the last seven days. A chart shows the current count and the count limit.

- **Licensing Report** shows the licensing history for each of the license types within the last seven days. The chart shows the current count and the count limit in a chart.
- **Licensing Report (All)** shows the licensing history for all the license types within the last seven days. A chart shows the current count and the count limit for each of the license types.
- **Storage Licensing Report** shows an overview of the storage used by the system for each day, with a breakdown of the raw event data size sent by each connector and by connector type.

ESM User Sessions

The ESM User Sessions use case provides information about user access to the ArcSight system. No configuration is required for this use case.

Using the ESM User Sessions Use Case

The **ESM User Sessions** use case is located in /All Use Cases/ArcSight Administration/ESM on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor user access to ArcSight ESM (user login and logout activity, including login session and notification information) and several reports that provide a historical view of ArcSight user login and logout activity. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- **ArcSight User Status** displays information about ArcSight Manager user sessions, including the username, the IP address and zone for the system from which the user is connecting, and the status of the connection (Logged In, Logged Out, or Login Timed Out).
- **ArcSight User Activity** displays information about the users currently logged into the ArcSight ESM system, such as the username, IP address of the system from which the user is connecting, the client type and version, and the last access time. Recent user session information and notification activity generated by ArcSight ESM rules are also provided.

Running Reports

The **ESM User Sessions** use case provides several reports that show information about ESM user sessions. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ArcSight User Login Trends** shows a summary of the number of ArcSight user logins for the previous day. A bar chart shows the total number of logins by user and a table shows the number of logins by user per hour.
- **ArcSight User Logins - Last Hour** shows details for all the ArcSight user logins within the past hour. The report contains a table showing the source host, the username, and the login time.
- **User Login Logout Report** shows successful and failed user login events, and logout events.

Actor Configuration Changes

The Actor Configuration Changes use case provides information about changes to the actor resources. No configuration is required for this use case.

Using the Actor Configuration Changes Use Case

The **Actor Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/ESM/Configuration Changes on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor changes made to the actor resources. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.

Viewing the Dashboards

The **Actor Configuration Changes** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Actor Administration** displays a list of all the authenticators for actors.
- **Actor Change Log** displays an overview of the actor resource changes (the total number of changes by type within the last hour) and the most recent events related to changes in actors (including creation, deletion, and modification of single-value and multi-value parameters of actor resources).

Viewing the Active Channel

To view the **Actor Audit Events** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events where there are data changes to the actor resources.

Running Reports

The **Actor Configuration Changes** use case provides several reports that give you a historical view of the changes made to the actor resources. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actor Full Name and Email Changes** shows information from actor audit events that result from changes to the Full Name or Email attribute of an actor. The report shows the old and new information.
- **Actor Manager and Department Changes** shows information from actor audit events that result from changes to the Department or Manager attribute of an actor. This report shows the old and the new information.
- **Actor Title and Status Changes** shows information from actor audit events that result from changes to the Title or Status attribute of an actor. The report shows the old and new information.
- **Configuration Changes by Type** shows recent actor configuration changes. A table lists all the changes grouped by type and user, and sorts them chronologically.
- **Configuration Changes by User** shows recent actor configuration changes. A table lists all the changes grouped by user and type, and sorts them chronologically.
- **Created** shows a list of all the actors created the previous day.
- **Deleted** displays audit event information for actors that have been deleted.
- **IDM Deletions of Actors** shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system.
- **Updated** shows a list of all the actors updated the previous day.

ESM Resource Configuration Changes

The ESM Resource Configuration Changes use case provides information about changes to the ESM resources, such as rules, reports, and so on. No configuration is required for this use case.

Using the ESM Resource Configuration Changes Use Case

The **ESM Resource Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/ESM/Configuration Changes on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor all changes to content resources and several reports that provide information about recently deleted, created, or updated ESM resources. The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

Viewing the Dashboard

To view the **Resource Change Log** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the total number of ESM resource changes by type within the last hour in a pie chart. Detailed information about logs associated with these changes is also provided.

Running Reports

The **ESM Resource Configuration Changes** use case provides several reports that provide historical information about recently deleted, created, or updated ESM resources. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ESM Configuration Changes by Type** shows recent ESM configuration changes. A table lists all the changes grouped by type, sorted chronologically. Use this report to find all the configuration changes of a certain type.
- **ESM Configuration Changes by User** shows recent ESM configuration changes. A table lists all the changes grouped by user, sorted chronologically. Use this report to find all the configuration changes made by a specific user.
- **Resource Created Report** shows a list of all the resources created by ESM users the previous day.
- **Resource Deleted Report** shows a list of all the resources deleted by ESM users the previous day.
- **Resource History Report** shows a list of all the resources that have been created, updated, or deleted by ESM users the previous day.
- **Resource Updated Report** shows a list of all the resources updated by ESM users the previous day.

Content Management

The Content Management use case provides resources that show information about content package synchronization with the ESM Content Management feature. The information includes the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.



Note: The Content Management use case is available only if you install the optional ArcSight Content Management package located in the ArcSight Administration package group.

For information about the ESM Content Management feature, refer to the [Command Center User's Guide](#).

Configuring the Content Management Use Case

Enable the **Content Management Data** rule. This rule maintains the **Content Management History** active list. To enable the rule, right-click the rule in the Rules section of the Content Management use case and select **Enable Rule**.

Enable the **Content Management Data Failure** rule. This rule sends a notification to the **Content Management** notification group each time a failure event occurs. Also, this rule maintains the **Content Management History Failure** active list. To enable the rule, right-click the rule in the Rules section of the Content Management use case and select **Enable Rule**.

To create a notification group for Content Management see the [ArcSight Console User's Guide](#).

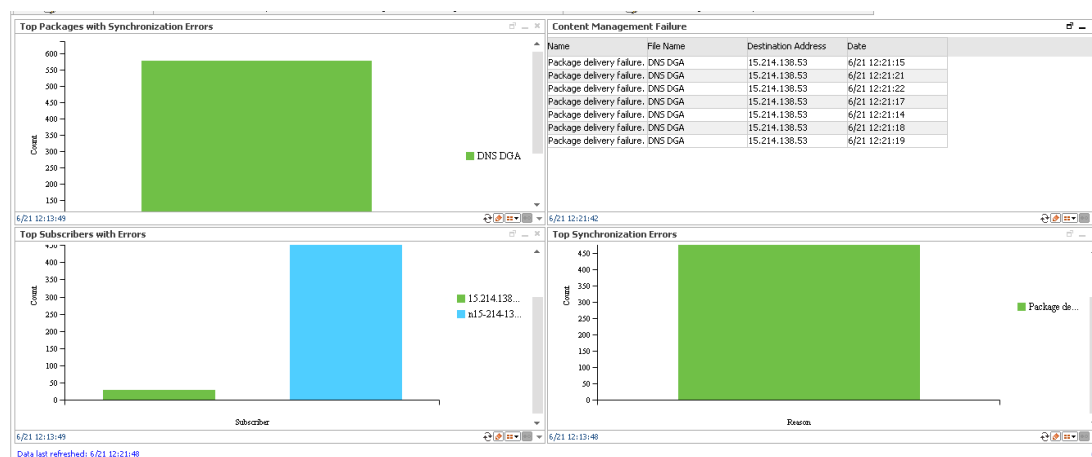
Using the Content Management Use Case

The **Content Management** use case is located in /All Use Cases/ArcSight Administration/ESM/Content Management on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor the history of content packages synchronized across peered ArcSight Manager or subscribers. Several reports provide a history of content package synchronization and information about content packages with synchronization errors or subscription errors. The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

Viewing the Dashboard

To view the **Synchronization Status History** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel as shown below:



The **Synchronization Status History** dashboard shows the following:

- The content packages with the most issues related to either package update delivery or installation after the package has been delivered.
- The most common issues with delivery or installation of managed packages.
- The subscribers experiencing the most issues with managed package delivery or installation.
- The Content Management failure events that have occurred recently.

Running Reports

The **Content Management** use case provides several reports that provide a historical view of the content package synchronization history and information about content packages with synchronization errors or subscription errors. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Top Packages with Synchronization Errors** shows information about the content packages with the most update delivery issues or installation issues after the package has been delivered.
- **Synchronization Status History** shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.
- **Top Synchronization Errors** shows information about the most common issues experienced by subscribers with managed package delivery or installation.
- **Top Subscribers with Errors** shows information about the subscribers experiencing the most issues with managed package delivery or installation.

Transformation Hub Monitoring

The Transformation Hub Monitoring optional package provides resources to help you monitor the status of connectivity and event consumption by ESM from a Transformation Hub deployment.

After Transformation Hub and connectors are properly configured for connectivity and topic identification, ESM can consume topics from Transformation Hub.

Prerequisites:

Using the resources from the Transformation Hub Monitoring package assumes that your environment has a deployment of Transformation Hub, and Transformation Hub is set up with one topic specifically for ESM consumption.

See the *Micro Focus Security ArcSight Data Platform Transformation Hub Administrator's Guide* and the accompanying *Release Notes*.

Transformation Hub Monitoring Audit Events

The Transformation Hub Monitoring content uses information from the Transformation Hub audit events generated by the ArcSight Manager.

The Device Event Class ID and Name fields, with more fields in the audit event are displayed in the Transformation Hub Audit Events active channel. See "[Viewing the Active Channel](#)" on [page 59](#).

The following table lists the Transformation Hub audit events.

Transformation Hub Audit Events

Device Event Class ID	Audit Event Description
thub:100	Connection to Transformation Hub is up
thub:101	Connection to Transformation Hub is down
thub:102	Number of messages remaining in Transformation Hub
thub:103	Number of events forwarded from Transformation Hub to ESM

Using the Transformation Hub Monitoring Use Case

The **Transformation Hub Monitoring** use case is an optional module installed in /All Use Cases/ArcSight Administration/ESM/Transformation Hub Monitoring on the **Use Cases** tab of the Navigator.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard and an active channel to help you monitor the status of Transformation Hub activity in terms of events received by ESM, and status of connectivity between ESM and Transformation Hub.

The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

Viewing the Dashboard


Launch the Transformation Hub Monitoring dashboard either from the use case, or from the Console's Resources Navigator:

- On the Transformation Hub Monitoring use case, click the Dashboards link, **Transformation Hub Monitoring**:
- On the Navigator Resources panel, expand /All Dashboards/ArcSight Administration/ESM/Transformation Hub Monitoring.
 - Right-click **Transformation Hub Monitoring** and select **Show Dashboard**, or
 - Double-click **Transformation Hub Monitoring**.



Note: If you change the Transformation Hub host information in the Manager, it will take 24 hours before the host information is completely updated on the data monitors. Query viewer information on hourly EPS rate is up to date because it is refreshed every 15 minutes.

The dashboard includes:

Data Monitors	<ul style="list-style-type: none">• Transformation Hub Status This is a Last State data monitor. A green circle indicates that ESM is connected to the Transformation Hub host. If the connection is broken, you should investigate if the Transformation Hub host itself is up.• Message Count Remaining in Transformation Hub This is a Last State data monitor. It indicates that there are messages in Transformation Hub that are yet to be consumed by ESM. If the circle is green, the message count is within acceptable thresholds.
Query Viewer	<p>Hourly EPS Forwarded from Transformation Hub</p> <p>The query viewer displays the total events per second consumed from Transformation Hub, every hour. It is refreshed every 15 minutes. If you want to update the data manually, click the Refresh button .</p>

Viewing the Active Channel

Launch the Transformation Hub Audit Events active channel either from the Transformation Hub Monitoring use case, or from the Console's Resources Navigator:

- On the Transformation Hub Monitoring use case, click the Active Channels link, **Transformation Hub Audit Events**:
- On the Navigator Resources panel, expand /All Active Channels/ArcSight Administration/ESM/Transformation Hub Audit Monitoring.
 - Right-click **Transformation Hub Audit Events** and select **Show Active Channel**, or
 - Double-click **Transformation Hub Audit Events**.

The Device Event Class ID and Name are among the columns of information displayed on this channel. The Source columns (address and hostname) correspond to the Transformation Hub host, while the Destination columns correspond to the ESM consumer.



Tip: Under Device Event Class ID, look for thub:101, which corresponds to the event name Connection to Transformation Hub is down. If not followed by thub:100, which corresponds to Connection to Transformation Hub is started, contact your Transformation Hub administrator to investigate and fix the connection problem.

Active Passive High Availability Monitoring

The Active Passive High Availability (APHA) Monitoring use case lets you monitor the status of ESM systems that are using the optional ESM Active Passive High Availability Module (APHA Module). The APHA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.

The APHA Monitoring use case is part of the optional ArcSight ESM APHA Monitoring content package. This content package is not installed by default on the ArcSight Manager. If you are using the APHA Module, you can opt to install the content package during ArcSight Manager installation or from the ArcSight Console any time after installation (right click the **ArcSight ESM APHA Monitoring** package in the ArcSight Administration folder on the **Packages** tab in the Navigator and select **Install Package**).

The APHA Monitoring use case provides several resources that help you monitor APHA events. You can see the current APHA status, the current Primary System, all ESM System status changes within the last 24 hours, and the last ten APHA status changes.

The APHA Monitoring content shows you general APHA status information and alerts you to problems. For more detailed diagnostics and troubleshooting, refer to the [ESM Active Passive High Availability Module User's Guide](#).



Note: The APHA Monitoring content displays data only if you have installed the APHA Module and you have set up APHA according to the [ESM Active Passive High Availability Module User's Guide](#).

Important: The APHA Monitoring active channel shows historical data (events generated since ArcSight Manager installation). The APHA Monitoring dashboard displays the current status (events arriving in real time). If you install the ArcSight ESM APHA Monitoring content package after ArcSight Manager installation, when the APHA link is established and fully in sync, the APHA Monitoring dashboard does not display the current OK status if no new APHA events are being generated.

APHA Monitoring Audit Events

The APHA Monitoring content uses information from the APHA audit events generated by the ArcSight Manager. The Device Event Class ID, Event Name, and Event Message fields in the audit event are displayed in the **APHA Monitoring** active channel and the **ESM APHA Status** dashboard. The **ESM APHA Status** dashboard provides the current APHA status, which is derived from the audit event fields. In most cases, the current APHA status and the Event Name field of the APHA audit event are identical.

The **APHA Monitoring** active channel and the **ESM APHA Status** dashboard are described in [Using the APHA Monitoring Use Case](#)

The following table lists the APHA audit events.

Device Event Class ID	Event Name	Event Message
highavailability:100	Primary Manager Started	Manager started up due to APHA failover or restart
highavailability:200	APHA Status Failed	APHA system failure
highavailability:300	DRBD Sync in Progress	Secondary system data syncing in progress Note: DRBD is the Distributed Replicated Block Device.
highavailability:400	iPDU status Failed	iPDU failover control function failed: iPDU agent stopped or cannot communicate with iPDU Note: iPDU is the Intelligent Power Distribution Unit.
highavailability:500	APHA Status OK	APHA system restored

Configuring the APHA Monitoring Use Case

The APHA Monitoring use case includes the **Alert - APHA Status Change** rule. This rule triggers when an APHA status change event (APHA audit event) is generated. After the rule triggers, a notification is sent to the SOC Operators team. Make sure that you have configured notification destinations so that the correct SOC operators are notified when an APHA status event is generated. For details on how to configure notification destinations, refer to the [ArcSight Console User's Guide](#).

Using the APHA Monitoring Use Case

The **APHA Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/APHA Monitoring on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

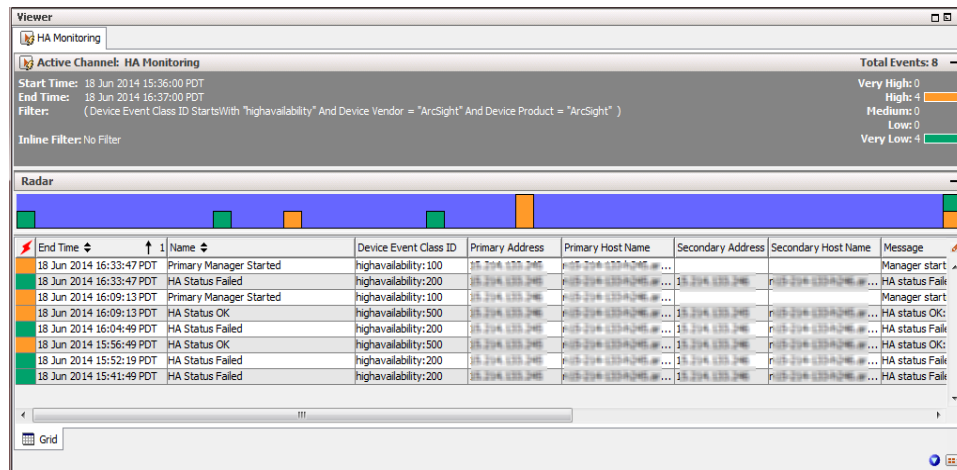
The Monitor section of the use case provides a dashboard, an active channel and a report to help you monitor the status of ESM systems using the optional ESM APHA Module. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channel, and report.


Viewing the Active Channel

To view the **APHA Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all APHA status events received within the last hour, including information such as when the Primary Manager started, when APHA failed, and when APHA returned to an OK state.

The active channel shows detailed information about the APHA audit events generated by the ArcSight Manager, such as the Device Event Class ID, the Event Name, the Event Message, and other information. The IP address and hostname of both the Primary System and Secondary System are also shown. See [APHA Monitoring Audit Events](#) for a list of the audit events generated by the ArcSight Manager.

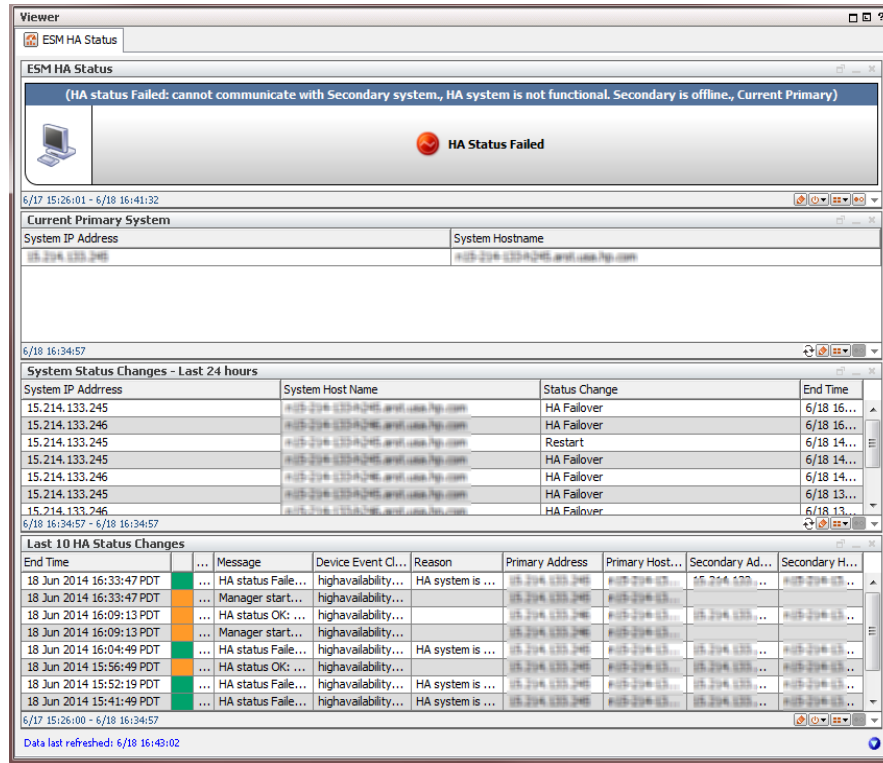
An example of the **APHA Monitoring** active channel is shown below.



 **Tip:** Double-click an event in the active channel to see details about the event in the Event Inspector.


Viewing the Dashboard

To view the **ESM APHA Status** dashboard, click the link for the dashboard start in the use case. The dashboard opens in the Viewer panel and displays an overview of the ArcSight ESM Active Passive High Availability (APHA) state.



The dashboard data monitors and query viewers are described below.

- The **ESM APHA Status** data monitor shows the current APHA status (such as APHA Status Failed or APHA Status OK). The Event Message and event reason from the latest audit event generated by the ArcSight Manager provide additional details and are also displayed at the top of the data monitor.

 **Tip:** To find out details about the current Primary System, such as the system hostname, IP address, and start time, click the data monitor heading. When the data monitor heading changes color, right click anywhere in the data monitor and select **Drilldown > Current Primary System**.

To generate a report showing all APHA status updates within the last seven days, right click anywhere in the data monitor and select **Drilldown > ESM APHA Status - last 7 days**.

The following table describes each APHA status alert shown in the middle of the **ESM APHA Status** data monitor and provides a description for each, including general troubleshooting tips. [APHA Monitoring Audit Events](#) provides a list of the APHA Monitoring audit events and includes the Device Event Class ID, Event Name, and Event Message fields for each event. The current APHA status is generated from the audit event fields.

ESM APHA Status	Description
APHA Status Failed	<p>The Secondary System has become unavailable and cannot assume the role of the Primary System. The audit event is generated every five minutes until the Secondary System is restored.</p> <p>Investigate the failure. Possible causes are:</p> <ul style="list-style-type: none"> • Failure of either network interface card (NIC) • Cross-over cable failure or disconnect • Secondary System failure or shutdown • Secondary System hard drive failure • Secondary System reboot • ArcSight ESM license expired
APHA Status OK	<p>The Secondary System has changed from APHA Status Failed to APHA Status OK. It might take 30 seconds for the audit event to generate after the Secondary System and high-availability service is restored.</p>
APHA Status Unknown	<p>There is a failover and the Secondary System has taken over to become the Primary System, or the Primary System has restarted. This status indicates two situations:</p> <ul style="list-style-type: none"> • The Primary System was restarted but no APHA failover occurred. • APHA failover occurred and the former Secondary System started up as the Primary System. <p>This status turns into either "APHA Status OK" or "APHA Status Failed" a few minutes after the Primary System starts up.</p>
DRBD Sync in Progress	<p>The Distributed Replicated Block Device (DRBD) storage system began the process of synchronizing the Primary and Secondary System hard drives, and continues every five minutes until synchronization is complete. Each audit event includes the amount of data between the two systems that has been synchronized as a percentage until it reaches 100 percent.</p> <p>Note: This status is typically short. The system detects the APHA status as soon as the Primary System starts up.</p>
iPDU status Failed	<p>The Intelligent Power Distribution Unit (iPDU) agent cannot communicate with the iPDU on either the Primary or Secondary System. The audit events are sent once every five minutes until communication is re-established. After the iPDU status returns to UP, you see the status APHA Status OK.</p>

- The **Current Primary System** query viewer shows the IP address and hostname of the current Primary System. Right click on the entry in the table and select **Drilldown > System Status Changes** to see all status changes for the System.

- The **System Status changes - Last 24 Hours** query viewer shows System changes, such as restarts and failovers, within the last 24 hours.
- The **Last 10 APHA Status Changes** data monitor shows the last ten APHA status changes. Right-click on an entry in the table and select **Drilldown > System Status Changes** to see all status changes for the selected System.

Running the Report

The APHA Monitoring use case provides the **ESM APHA Status Updates - last 7 days** report. Run this report to see all APHA status updates within the last seven days. You can provide this historical report to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.



Tip: You can also run the report from the **ESM APHA Status** data monitor of the **ESM APHA Status** dashboard by right-clicking the data monitor heading and selecting **Drilldown > ESM APHA Status - last 7 days**.

ESM Events

The ESM Events use case provides statistics on the flow of events through the ArcSight system. No configuration is required for this use case.

Using the ESM Events Use Case

The **ESM Events** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several dashboards to help you monitor your ArcSight ESM and non-ArcSight ESM events (including event throughput), active channels that show system monitoring events generated by the local ArcSight ESM system and all events generated by ArcSight, and reports that provide historical information about ArcSight events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

Viewing the Dashboards

The **ESM Events** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Event Count History** displays the total number of non-ArcSight ESM events within the last seven days and within the last 30 days.
- **Event Overview** displays an overview of non-ArcSight ESM events focusing on event counts, events by connector, by vendor and product, and by device IP address.
- **Event Throughput** displays event throughput information in addition to an overview of the system activity related to connectors.
- **Latest Events By Priority** displays event count distribution by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.

Viewing the Active Channels

The **ESM Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.

- **ASM Events** shows ArcSight System Monitoring events generated by the local ArcSightESM system.
- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.

Running Reports

The **ESM Events** use case provides several reports that show information about ArcSight events. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Destination Counts** shows destination details and the sum of event counts for each destination.
- **Event Count by Agent Severity** shows events by agent severity with event counts.
- **Event Count by Source Destination Pairs** shows event counts by source-destination pairs.
- **Event Name Counts** shows event names and their event counts.
- **Events by ArcSight Priority (Summary)** displays a table of all events, grouped by ArcSight priority, showing the count of each event occurrence within that priority. Note: This report shows all ArcSight events; use the `FilterBy` parameter to limit the output to the areas of most interest.
- **Hourly Distribution Chart for Event** shows the hourly distribution of specific events.
- **Hourly Distribution Chart for a Destination Port** shows the hourly distribution of events for destinations with a specific port.
- **Hourly Distribution Chart for a Source Port** shows the hourly distribution of events for sources with a specific port.
- **Hourly Event Counts (Area Chart)** shows the hourly distribution of event counts.
- **Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)** shows the hourly distribution of events by priority rating.

- **Source Counts by Event Name** shows event names by source address in addition to event counts.
- **Top 10 Events** shows the top events by count.
- **Top 10 Inbound Events** shows the top inbound events by count.
- **Top 10 Outbound Events** shows the top outbound events by count.

ESM Reporting Resource Monitoring

The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers. No configuration is required for this use case.

Using the ESM Reporting Resource Monitoring Use Case

The **ESM Reporting Resource Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards, active channels, and reports to help you monitor, investigate and report on performance statistics for reports, trends, and query viewers. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

Viewing the Dashboards

The **ESM Reporting Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Query Running Time Overview** shows the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by query type.
- **Query Viewer Details** shows query details for query viewers.
- **Report Details** shows query details for reports.
- **Reporting Subsystem Statistics** shows an overview of the resources and processing time devoted to reports.
- **Trend Details** shows query details for trends.

Viewing the Active Channels

The **ESM Reporting Resource Monitoring** use case provides three active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Query Viewer Status** shows all the query viewer-related events received within the last two hours.
- **Reports Status** shows all the report-related events received within the last two hours.

- **Trends Status** shows all the trend-related events within the last two hours. The Trend Name field shows the name of the Trend and the URI. The Trend Infos field shows information on the Trend event.

Running Reports

The **ESM Reporting Resource Monitoring** use case provides several reports that show information about queries. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Failed Queries** shows the failed queries for trends, reports, and query viewers made within the past week.
- **Longest QueryViewer Queries** shows query duration information for query viewers made during the past week. A chart shows the top ten longest queries for a query viewer and a table shows the duration details for query viewers.
- **Longest Report Queries** shows query duration information for reports made during the past week. The chart shows the ten longest report queries and the table shows the duration details for the report queries.
- **Longest Trend Query** shows query duration information for trends made during the past week. A chart shows the ten longest trend queries and a table shows the duration details for trend queries.
- **Query Counts by Type** shows the number of queries made within the past week, grouped by type.

ESM Resource Monitoring

The ESM Resource Monitoring use case provides processing statistics for various resources, such as trends, reporting, rules, and data monitors.

Configuring the ESM Resource Monitoring Use Case

Enable the notification action for the following rules, if appropriate for your organization:

- **Excessive Rule Recursion**
- **Rule Matching Too Many Events**

For information about how to enable notification actions, see the [ArcSight Console User's Guide](#).

Using the ESM Resource Monitoring Use Case

The **ESM Resource Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards that show statistics about the rules engine, reporting, queries used for reports and trends, and data monitors.

Also, reports are provided to show information about the resources being used by your ESM system. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

The **ESM Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

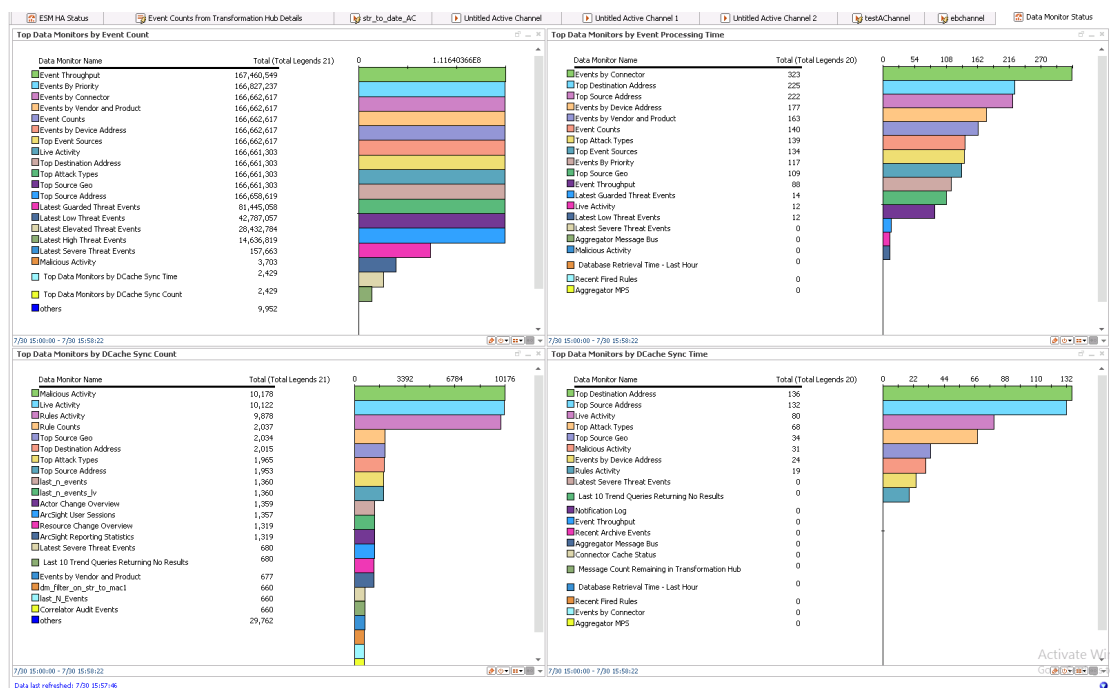
- **Query Running Time Overview** displays the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by type and query failures during the last 24 hours.
- **Reporting Subsystems Statistics** displays an overview of the resources and processing time devoted to reports.

- **Rules Status** displays information about the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, and error logs are shown.



Note: The Sortable Rules Stats data monitor on the Rules Status dashboard does not include pre-persistence rules.

- **Data Monitor Status** displays information about the load and performance of data monitors. The dashboard provides information about the top data monitors based on event count, event processing time, distributed cache synchronization count, and distributed cache synchronization time. Data Monitors that cause unusual load on the system and reduce event throughput are likely to be displayed on this dashboard. The Data Monitor Status Dashboard is shown below:



Note: Data monitors based on distributed cache synchronization data are visible only when ESM is used in distributed mode.

Running Reports

The **ESM Resource Monitoring** use case provides several reports that show information about the resources being used by your ESM system. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Active List Access** shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries the previous day, grouping the counts by ten-minute intervals. A table shows details of the active list access, grouping the number by time interval and active list name.
- **Correlation Events Statistics** shows information about correlation events. A chart shows the number of correlation events within the last hour, grouping them by ten-minute intervals. A table shows details of the number of correlation events, grouping them by rule name and time interval.
- **Data Monitor Evaluations Statistics** shows a chart with the average number of data monitor evaluations per second.
- **Fired Rule Events** shows all events that were triggered by a rule (correlation events) and includes the number of times the rule triggered and the ESM priority of the event.
- **Invalid Resources** shows a list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI.
- **Number of Events Matching Rules** shows the total number of events matching rules within the last hour, grouping them by ten-minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both rule types.
- **Rules Engine Warning Messages** shows warning messages received from the rules engine during the past 24 hours.
- **Session List Access** shows session list access statistics. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by ten-minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name.
- **Top Accessed Active Lists** shows the top ten accessed active lists. A chart shows the top ten accessed active lists the previous day, grouping the counts by ten-minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval.

- **Top Accessed Session Lists** shows the top ten accessed session lists. A chart shows the top ten accessed session lists within the last hour, grouping the counts by ten-minute intervals. A table shows details of the session list access, grouping the number by active list name and time interval.

ESM Storage Monitoring (CORR-Engine)

The ESM Storage Monitoring (CORR-Engine) use case provides information on the health of the CORR (Correlation Optimized Retention and Retrieval)- Engine.

No configuration is required for this use case.

Using the ESM Storage Monitoring (CORR-Engine) Use Case

The **ESM Storage Monitoring (CORR-Engine)** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and reports to help you monitor and report on database performance and the status of the database archive, including critical archive failures and archive task failures. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

Viewing the Dashboards

The **ESM Storage Monitoring (CORR-Engine)** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Active Status** displays database archive information.
- **Database Performance Statistics** displays an overview of database related statistics, such as available space, insert, and retrieval times.

Running Reports

The **ESM Storage Monitoring (CORR-Engine)** use case provides several reports that show information about the ESM Storage Monitoring (CORR) engine. You can provide these historical reports to the stakeholders in your company, when needed.

To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Event Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC_EVENT_DATA database table space for the last 30 days.
- **System Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC_SYSTEM_DATA database table space for the last 30 days.
- **ASM Database Free Space** shows the current free space percentages for the ASM database table spaces. The report shows the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.
- **ASM Database Free Space - by Day** shows the free space percentages by day for each of the ASM database table spaces. The report has one chart and one table, and has a custom parameter that can be used to choose one of the table spaces.
- **ASM Database Free Space - by Hour** shows the free space percentages by hour for the ASM database table spaces. The report shows the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.
- **Archive Processing** shows the archives that take the longest to process and the time it takes to archive information.
- **Archive Status Report** shows the current status of archive and disk space used.

Logger Events

The Logger Events use case provides statistics for events sent through a Logger. No configuration is required for this use case.

Using the Logger Events Use Case

The **Logger Events** use case is located in /All Use Cases/ArcSight Administration/Logger on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two active channels to help you investigate Logger application and platform events. The Library section of the use case lists supporting resources that help compile information in the active channels.

Viewing the Active Channels

The **Logger Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Logger Application Events** shows all the Logger application events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.
- **Logger Platform Events** shows all the Logger platform events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.

Logger System Health

The Logger System Health use case provides performance statistics for any Logger connected to the ArcSight system.

Configuring the Logger System Health Use Case

If you have a Logger connected to the ArcSight system, configure the Logger System Health use case for your environment as follows:

1. Enable the following rules in the /All Rules/Real-time Rules/ArcSight Administration/Logger/System Health folder:
 - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
 - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensors statuses for the same sensor type for a Logger indicate OK.
 - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

For information about enabling rules, refer to the [ArcSight Console User's Guide](#).

2. Edit the **My Logger** filter in the /All Filters/ArcSight Administration/Logger/System Health folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.
3. Enable the following data monitors:
 - a. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory folder:
 - **CPU Usage (Percent) - Last 10 Minutes**
 - **CPU Usage (Percent) - Last Hour**
 - **Memory Usage (Mbytes per Second) - Last 10 Minutes**
 - **Memory Usage (Mbytes per Second) - Last Hour**
 - b. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware folder:

- **CPU Sensors**
 - **FAN Sensors**
 - **System Sensors**
- c. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview folder:
- **Sensor Type Status**
- d. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Network folder:
- **EPS Usage (Events per Second) - Last 10 Minutes**
 - **EPS Usage (Events per Second) - Last Hour**
 - **Network Usage (Bytes) - Last 10 Minutes**
 - **Network Usage (Bytes) - Last Hour**
- e. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage folder:
- **Disk Read and Write (Kbytes per Second) - Last 10 Minutes**
 - **Disk Read and Write (Kbytes per Second) - Last Hour**
 - **Disk Usage (Percent)**

For information about data monitors, refer to the *Enabling or Disabling a Data Monitor* section in the [ArcSight Console User's Guide](#).

Using the Logger System Health Use Case

The **Logger System Health** use case is located in /All Use Cases/ArcSight Administration/Logger on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and an active channel to help you monitor and investigate the health of the Logger system defined in the **My Logger** filter. The Library section of the use case lists supporting resources that help compile information in the dashboards and active channel.

Viewing the Dashboards

The **Logger System Health** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **CPU and Memory** shows the CPU and memory usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.
- **Hardware** shows the status for all the hardware sensors on the Logger defined in the My Logger filter. The dashboard includes the CPU Sensors, FAN Sensors, and System Sensors data monitors.
- **My Logger Overview** shows an overview of the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the **My Logger** filter.
- **Network** shows the network and EPS usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.
- **Storage** shows the disk usage and the disk read/write speed within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.

Viewing the Active Channel

The **Logger System Health** use case provides the **Logger System Health Events** active channel, which shows all Logger system health events received within the last hour. To view the active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.

Chapter 4: ArcSight Foundation Content

The ArcSight Foundation content contains Shared Libraries, which are common resources that provide core functionality for common security scenarios. It also contains the resources that you can install with the Manager.

The ArcSight Foundation use cases are listed in the table below.



Note: When you perform a new ArcSight Manager installation, the ArcSight Foundation content packages are installed automatically. However, package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

Use Case	Purpose
Security Threat Monitoring	
Security Threat Monitoring	This use case contains the default security threat monitoring content.
Threat Intelligence Platform	
Threat Intelligence Platform	This use case contains resources that detect security attacks based on a threat intelligence feed.
MITRE ATT&CK Overview	
MITRE ATT&CK Overview	This use case contains resource for MITRE ATT&CK.
ArcSight ESM SOAR Integration	
ArcSight ESM SOAR Integration	This use case contains resources for integration ESM with SOAR.

Security Threat Monitoring

The Security Threat Monitoring package monitors security threats based on security log events from the firewall, IDS/IPS, OS, Application, Scanner, Anti-Virus, and cloud applications. This package follows the MITRE ATT&CK frame work and resources are organized by use case. Security Threat Monitoring provides filters, rules, data monitors, dashboards, active lists, active channels, fields, field sets, queries, query viewers, and use cases to help you monitor events in your system.



Note: Security Threat Monitoring is a required package and is automatically installed when you install ESM.

Resource Locations:

Note that each group of resources is then further organized by use case. For example, /All Rules/ArcSight Foundation/Security Threat Monitoring/<Malware Monitoring>/Registry Injection.

- Filters: /All Filters/ArcSight Foundation/Security Threat Monitoring.
- Rules: /All Rules/ArcSight Foundation/Security Threat Monitoring.



Note: To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

- Data Monitors: /All Data Monitors/ArcSight Foundation/Security Threat Monitoring.
- Dashboards: /All Dashboards/ArcSight Foundation/Security Threat Monitoring.
- Active Lists: /All Active Lists/ArcSight Foundation/Security Threat Monitoring.
- Active Channels: /All Active Channels/ArcSight Foundation/Security Threat Monitoring.
- Fields: /All Fields/ArcSight Foundation/Security Threat Monitoring.
- Field Sets: /All Field Sets/ArcSight Foundation/Security Threat Monitoring.
- Queries: /All Queries/ArcSight Foundation/Security Threat Monitoring.
- Query Viewers: /All Query Viewers/ArcSight Foundation/Security Threat Monitoring.
- Use Cases: /All Use Cases/ArcSight Foundation/Security Threat Monitoring.

Click [here](#) to see the full list of Security Threat Monitoring resources. For more information on the supported use cases, tactics, and techniques, see [ESM Default Content on the ArcSight Marketplace](#) and the [MITRE ATT&CK Navigator](#).

Configuring the Security Threat Monitoring Use Case

To configure the Security Threat Monitoring master use case:

1. Navigate to the **Security Threat Monitoring** use case present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.
2. Double click on the **Security Threat Monitoring** use case. The **Security Threat Monitoring** use case opens in the Viewer panel.
3. On the **Security Threat Monitoring** use case Viewer panel, under the Library section, you can see the active lists and fields. Under the Toolbox section, you can see the child use cases.
4. Click Configure, present just above the Monitor section, to configure the **Security Threat Monitoring** use case. A configuration wizard to guide you through configuration tasks appears on your screen.
5. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.
6. Click Next. The wizard takes you to the Categorize Protected Zones screen. Select the zones that contain internal network assets to categorize them as Protected.
7. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
8. Click Next to save the configuration settings to the use case resources. The wizard takes you to the Configuration Complete screen.
9. Click Finish.

Configuring the Child Use Cases

The Security Threat Monitoring package has multiple child use cases. The child use cases for Security Threat Monitoring are given below:

Child Use Cases
Application Monitoring
<ul style="list-style-type: none">• Application Monitoring
Entity Monitoring

Child Use Cases
<ul style="list-style-type: none">• Account Activity• Brute Force Attacks• Unsuccessful User Logins
Host Monitoring
<ul style="list-style-type: none">• Host Monitoring
Malware Monitoring
<ul style="list-style-type: none">• Malware Monitoring
Network Monitoring
<ul style="list-style-type: none">• Attacks and Suspicious Activity Overview• Network Monitoring
Perimeter Monitoring
<ul style="list-style-type: none">• Perimeter Monitoring
Vulnerability Monitoring
<ul style="list-style-type: none">• Vulnerability Monitoring

For your reference, an example to configure the **Unsuccessful User Login** use case is given below.

The **Unsuccessful User Login** use case includes different resources to monitor the below unsuccessful login activities:

- Consecutive Unsuccessful Logins to Administrative Account.
- Consecutive Unsuccessful Logins to Same Account from different Countries.
- Consecutive Unsuccessful Logins to Same Account from different IPs.
- Multiple Failed Login to Different Accounts from Single Source.
- General Unsuccessful Logins.
- Failed Login count by user accounts, source and destination systems.



Note: If a rule is based on Windows Event ID 4688, ensure that the Audit Process Creation policy is enabled on the Microsoft system you want to monitor. For more information, see Microsoft's documentation.

To configure the Unsuccessful User Login use case:

1. Navigate to the following location in the ESM Console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Unsuccessful User

Login/.

2. Double click on the **Unsuccessful User Login** use case. The **Unsuccessful User Login** use case opens in the Viewer panel as shown below.
3. On the **Unsuccessful User Login** use case Viewer panel, under the Library section, you can see the associated active lists, data monitors, field sets, filters, and rules. Under the Monitor section, you can see the dashboards and active channels.
4. Click Configure, present just above the Monitor section, to configure the **Unsuccessful User Login** use case. A configuration wizard to guide you through configuration tasks appears on your screen.
5. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.
6. Click Next. The wizard takes you to the Confirm Event Sources screen. The possible event sources of this use case are listed on this screen. Ensure that at least one event source is configured with a connector and is sending events.
7. Click Next. The wizard takes you to the Privilege User Accounts Configuration screen. You can either import your privilege user accounts or enter the information manually.
8. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
9. Click Next to save the configuration settings to the use case resources. The wizard takes you to the Configuration Complete screen.
10. Click Finish.

Using the Security Threat Monitoring Use Case

The **Security Threat Monitoring** use case consists of a master use case and multiple child use cases.

The master use case is known as **Security Threat Monitoring** and is present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.

The child use cases for Security Threat Monitoring are present at the following location in the ESM Console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

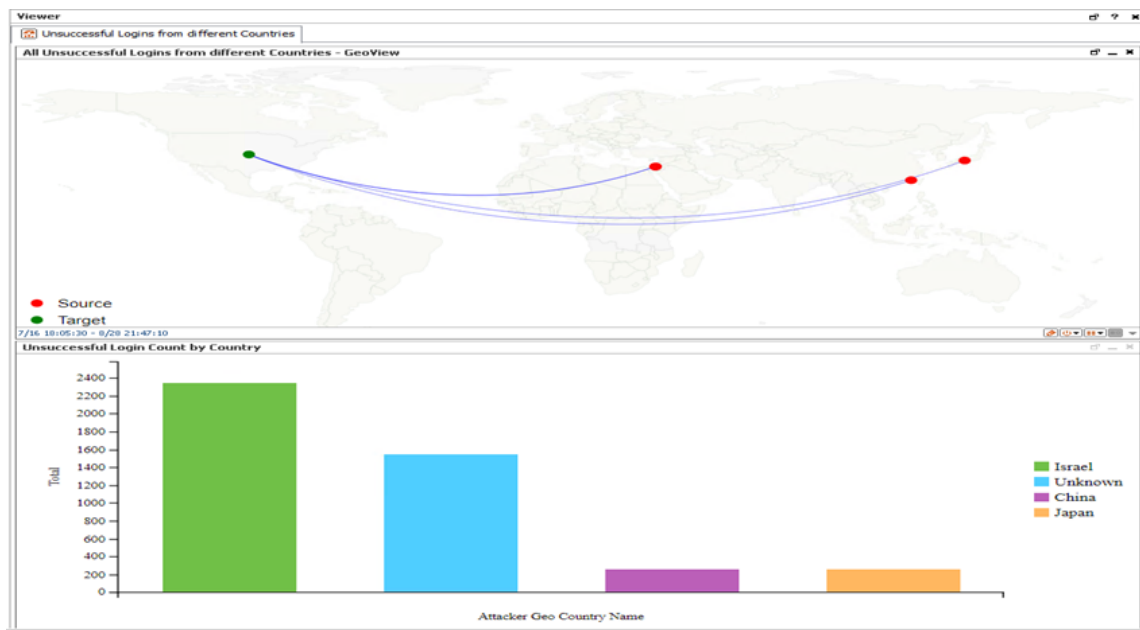
For your reference, an example to use the **Unsuccessful User Login** child use case is given below.

The **Unsuccessful User Login** use case is present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

Viewing the Dashboard

To view the **Unsuccessful Logins from different Countries** dashboard, click the link for the dashboard in the **Unsuccessful User Login** use case. The dashboard opens in the Viewer panel as shown below:



The **Unsuccessful Logins from different Countries** dashboard shows the following:

- All Unsuccessful Logins from different Countries - GeoView
- Unsuccessful Login Count by Country

Threat Intelligence Platform

The Threat Intelligence Platform package contains resources that detect security attacks based on a threat intelligence data feed. This package uses the Galaxy Threat Acceleration Program (GTAP) connector as a threat intelligence data feed. The threat intelligence data feed from GTAP is directly imported to ESM using the Model Import Connector (MIC). This package follows the MITRE ATT&CK frame work and resources are organized by use case. Threat Intelligence Platform provides filters, rules, data monitors, dashboards, active lists, active channels, fields, field sets, queries, query viewers, integration commands, and use cases to help you monitor events in your system.



Note: Threat Intelligence Platform is a required package and is automatically installed when you install ESM.

Resource Locations:

- Filters: /All Filters/ArcSight Foundation/Threat Intelligence Platform.
- Rules: /All Rules/ArcSight Foundation/Threat Intelligence Platform.



Note: To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

- Data Monitors: /All Data Monitors/ArcSight Foundation/Threat Intelligence Platform.
- Dashboards: /All Dashboards/ArcSight Foundation/Threat Intelligence Platform.
- Active Lists: /All Active Lists/ArcSight Foundation/Threat Intelligence Platform.
- Active Channels: /All Active Channels/ArcSight Foundation/Threat Intelligence Platform.
- Fields: /All Fields/ArcSight Foundation/Threat Intelligence Platform.
- Field Sets: /All Field Sets/ArcSight Foundation/Security Threat Monitoring.
- Queries: /All Queries/ArcSight Foundation/Security Threat Monitoring.
- Query Viewers: /All Query Viewers/ArcSight Foundation/Threat Intelligence Platform.
- Use Cases: /All Use Cases/ArcSight Foundation/Threat Intelligence Platform.

Click [here](#) to see the full list of Threat Intelligence Platform resources or to search for them by their specific URLs. For more information on the supported use cases, tactics, and techniques see [ESM Default Content on the ArcSight Marketplace](#) and [MITRE ATT&CK Navigator](#).

Configuring the Threat Intelligence Platform Use Case

To configure the Threat Intelligence Platform use case:

1. Navigate to the **Threat Intelligence Platform** use case present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Threat Intelligence Platform/.
2. Double click on the **Threat Intelligence Platform** use case. The **Threat Intelligence Platform** use case opens in the Viewer panel.
3. On the **Threat Intelligence Platform** use case Viewer panel, under the Library section, you can see the active lists, fields, filters, and rules. Under the Toolbox section, you can see the event sources and supporting tools. Under the Monitor section, you can see the dashboards and query viewers.
4. Click Configure, present just above the Monitor section, to configure the **Threat Intelligence Platform** use case. A configuration wizard to guide you through configuration tasks appears on your screen.
5. This configuration wizard guides you through the following configuration tasks: **Check for required event sources** and **Categorize zones you want to monitor**.
6. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.
7. Click Next. The wizard takes you to the Confirm Event Sources screen. The possible event sources of this use case are listed on this screen. Ensure that at least one event source is configured with a connector and is sending events.
8. Click Next. The wizard takes you to the Categorize Protected Zones screen. Select the zones that contain internal network assets to categorize them as Protected.
9. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
10. Click Next to save the configuration settings to the use case resources. The wizard takes you to the **Configuration Complete** screen.
11. Click Finish.

Using the Threat Intelligence Platform Use Case

The **Threat Intelligence Platform** use case is located at /All Use Cases/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Platform on the **Use**

Cases tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.



Note: For this use case, install MIC, which imports/updates MISP intelligence data into the Detect server. Also, define indicator types for each use case in the list /All Active Lists/ArcSight Foundation/Common/Suspicious Indicator Types .

Viewing the Dashboards

To view the dashboards, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.



Note: To view detailed information about each graphic view in the dashboards, use the drill-down feature present in each of the graphic views. To use the drill-down feature, right-click on the graphic view for which you want to view the detailed information.

MITRE ATT&CK Overview Use Case

All the rules in the [Security Threat Monitoring \(STM\)](#) and [Threat Intelligence Platform \(TIP\)](#) packages are assigned MITRE ATT&CK IDs, such as T1018, and are linked to a MITRE ATT&CK group. The MITRE ATT&CK use case contains resources that allows you to find, filter, and display results of the rules in the STM and TIP packages.

Resources

These resources can also be found organized by type in the [Security Monitoring Base appendix](#).

Active Lists:

/All Active Lists/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK List

/All Active Lists/ArcSight Foundation/MITRE ATT&CK/Rules Triggered with Mitre ID

Active Channel:

/All Active Channels/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK

Dashboards:

/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE Alerts Graph View

/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Overview

/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Targets Overview

Data Monitors:

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Last MITRE ATT&CK Events

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Alert Graph View

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Attackers and Targets Relations

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Fired MITRE ATT&CK Rules

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Target IPs

/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Target Users

Field Set:

/All Field Sets/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK

Fields:

/All Fields/ArcSight Foundation/MITRE ATT&CK/getMitre

/All Fields/ArcSight Foundation/MITRE ATT&CK/getTriggeredRule

/All Fields/ArcSight Foundation/MITRE ATT&CK/getTacticTriggeredRule

/All Fields/ArcSight Foundation/MITRE ATT&CK/mitreID

/All Fields/ArcSight Foundation/MITRE ATT&CK/mitreName

/All Fields/ArcSight Foundation/MITRE ATT&CK/taticName

Filters:

/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE Alerts

/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK with Attacker and Target

/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK

Integration Command and Configuration:

/All Integration Configurations/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Lookup

/All Integration Commands/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Lookup

Queries:

/All Queries/ArcSight Foundation/MITRE ATT&CK/Alert with Mitre ID Details

/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre by Id

/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre Details Summary

/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre by Tactic

Query Viewers:

/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/Alert with Mitre ID Details

/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/MITRE by ID

/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/MITRE by Tactic

Rule:

/All Rules/Real-time Rules/Track Rules triggered

ArcSight ESM SOAR Integration

The ArcSight ESM SOAR Integration package contains the following resources that allow you to integrate ESM with SOAR and select the alerts to forward to SOAR:

Resource	Type	Path	Description
SOAR Integration Rule	Pre-persistence rule	/All Rules/ArcSight Foundation/SOAR/	Sets the old hashfile to change_me for correlation events which should be forwarded to SOAR. Correlation events are defined in an active list.
SOAR Rule Names	Active list	/All Active Lists/ArcSight Foundation/SOAR/	Contains all rules which should be forwarded to the SOAR integration.
apiSOAR	Filter	/All Filters/ArcSight Foundation/SOAR/	Used by the SOAR Web user.
forwardSOAR	Filter	/All Filters/ArcSight Foundation/SOAR	Shows events to be forwarded to SOAR.
forwardSOAR	Active channel	/All Active Channels/ArcSight Foundation/SOAR	Shows events to be forwarded to SOAR.

For more information about integrating ESM with SOAR, see the [Administrator's Guide for the ArcSight Platform](#).

Chapter 5: ArcSight System Content

The ArcSight System content consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for default functionality. Resources that manage core functionality are **locked** to protect them from unintended change or deletion.

In this section, the ArcSight System resources are grouped together based on the functionality they provide. The ArcSight System resource groups are listed in the table below.

Resource Group	Purpose
"Actor Support Resources" on the next page	Includes resources that support the actors feature.
"Priority Formula Resources" on page 94	Includes resources that directly or indirectly affect the Priority Formula.
"System Resources" on page 96	Includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

Actor Support Resources

The actors feature maps people and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems, and correlating them with user account information from the user authentication systems in your network. Correlating user identifiers from the event traffic that reflects their activity throughout the day makes it possible to ensure that users are doing role-appropriate activity across the assets in your organization, and to detect and track inappropriate access and suspicious activity. For more information on Actors, see the [ArcSight Console User's Guide](#).



Note: Actors are a licensed feature; they do not apply to every environment.

Using the Actor Support Resources

The actor support resources consist of several reports located in the /All Reports/ArcSight System/Core/ folder on the **Resource** tab of the Navigator:

- **Actor Context Report by Target Username** shows activity related to an actor based on the ActorByTargetUserName global variable.
- **Actor Context Report by Account ID** shows activity related to an actor based on the ActorByAccountID global variable.
- **Actor Context Report by Attacker Username** shows activity related to an actor based on the ActorByAttackerUserName global variable.
- **Actor Context Report by Custom Fields** shows activity related to an actor based on the ActorByCustomFields global variable.

To run a report:

1. Right-click the report in the Navigator tree on the **Resource** tab and select **Run**.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

Priority Formula Resources

The Priority Formula Resources group includes resources that directly or indirectly affect the Priority Formula. The Priority Formula is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. The Priority Formula is also referred to as the Threat Level Formula. For more information about the Priority Formula, refer to the [ArcSight Console User's Guide](#) or [ESM 101](#).

There are no monitoring resources for the priority formula. However, there are several rules that detect successful hostile attempts and identify correlation events that originate from other reconnaissance rules. See "[Priority Formula Rules](#)" below.

Configuring the Priority Formula Resources Group

Configure the following active lists:

- Populate the **Trusted List** active list with the IP sources on your network that are known to be safe.
- Populate the **Untrusted List** active list with the IP sources on your network that are known to be unsafe.

For more information about working with active lists, see "[Configuring Active Lists](#)" on [page 16](#).



Note: You can set up rules to add and remove entries from the **Trusted List** and **Untrusted List** active lists dynamically. The information in these active lists is then used in the Priority Formula.

Priority Formula Rules

The Priority Formula resources consist of several rules located in the `/All Rules/ArcSight System/` folder on the **Resource** tab of the Navigator.

- **Reconnaissance - Attackers** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events from an attacker. The rule adds the attacker to the Reconnaissance List active list.
- **Reconnaissance - Targets** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events targeted by an external attacker to an internal asset. The rule adds the target information into the Scanned List active list.
- **Compromise - Success** detects any successful attempt to compromise a device from a source that is not listed in the Trusted List active list, with either the attacker information

(zone and address) or the target information present. The rule triggers whenever an event is categorized as Success and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List and Infiltrators List active lists, and the target address is added to the Compromised List and Hit List active lists.

- **Hostile - Attempt** detects any hostile attempt on a device that is not already compromised from a source that is not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Attempt and Hostile, and the target does not belong to a compromised active list.
- **Hostile - Success** detects any successful hostile attempts on a device that is not already compromised from a source not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Infiltrators List active list, the target address is added to the Compromised List active list, and the target information is removed from Hit List active list.
- **Compromise - Attempt** detects any attempt to compromise a device from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.
- **Incident Resolved - Remove From List** detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. This rule only triggers if you have the Intrusion Monitoring package installed from a previous ESM release.

System Resources

The System Resources group includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

Configuring System Resources

Configure the following filters:

- Modify the **Connector Asset Auto-Creation Controller** filter to specify which assets to exclude from the asset auto creation feature.
The **Connector Asset Auto Creation Controller** filter directs the creation of an asset for network nodes represented in events received from the connectors present in your environment. By default, the **Connector Asset Auto Creation Controller** filter is configured with the generic condition True, which matches all events. You can exclude connectors from a specific zone, such as a VPN zone, (where the asset already exists, but traffic is coming into the network from an alternate VPN interface). You can also exclude traffic from different types of connectors, such as from a particular device and vendor. For more information about asset auto creation, refer to the [ArcSight Console User's Guide](#).
- Modify the **Device Asset Auto-Creation Controller** filter.
ArcSight creates assets in the asset model automatically for events whose devices are not already modeled either manually or using an asset scanner. Depending on what devices you have reporting to ArcSight and what devices report in to your network, this can cause more individual assets to be added to your asset model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device. By default, the Device Asset Auto Creation Controller filter is configured with the generic condition True, which matches all events. Configure this filter to specify traffic from specific devices and device vendors, or event categories, such as Hostile. When you specify an event category, the filter directs the system to only create assets for events with this severity.
- Modify the **SNMP Trap Sender** filter if you have the SNMP Trap Sender enabled to forward events through SNMP to a network management system.
By default, this filter is configured with the /ArcSight System/Event Types/ArcSight Correlation Events filter. If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events are trapped and forwarded to the network management system.
To configure this filter to forward certain events as an SNMP trap, change the default condition in the SNMP Trap Sender filter to specify which events are forwarded as traps. You can express this condition directly in the SNMP Trap Forwarding filter, or you can

create another filter that expresses these parameters and point to it in the SNMP Trap Sender filter. To enable the SNMP trap sender, refer to the [Administrator's Guide](#).

Using the System Resources

The System Resources group consists of several active channels that show events received by ArcSight ESM over different periods of time, two reports that are used by the ArcSight console for internal processing, and several integration commands that you can use in ArcSight ESM active channels and dashboards.

Viewing the Active Channels

The System Resources group provides several active channels located in the `/All Active Channels/ArcSight System/` folder on the **Resource** tab of the Navigator. To open an active channel, right-click the active channel in the resource tree and select **Show Active Channel**. The active channels are described below:

- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.
- **Today** shows all events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events.
- **Last 5 Minutes** in `/All Active Channels/ArcSight System/All Events` shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.
- **Last Hour** in `/All Active Channels/ArcSight System/All Events` shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data.
- **Live** in `/All Active Channels/ArcSight System/Core` shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.
- **Personal Live** in `/All Active Channels/ArcSight System/Core` shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events. This active channel also hides all the events that have been assigned to the current user.

Reports

The System Resources group consists of two reports located in the /All Reports/ArcSight System/Core/ folder on the **Resource** tab of the Navigator:

- **Assets having Vulnerabilities** is used by the ArcSight Console for internal processing; do not run this locked report.
- **Selected Case Report** is a basic report template for case management. Refer to the [ArcSight Console User's Guide](#) topic on "Creating a Report on a Case."
- **Vulnerabilities of an Asset** is used by the ArcSight Console for internal processing; do not run this locked report.

Integration Commands

ArcSight ESM provides several integration commands; a set of tools that make it possible to invoke scripts and utilities directly from the ArcSight Console. You can use these commands directly from dashboards and active channels. You can edit these commands from the /All Integration Commands/ArcSight System/Tools folder in the Resource tree of the Navigator panel.

- **Nslookup (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find details about an IPv4 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.
- **Nslookup-IPV6 (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find details about an IPv6 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.
- **Nslookup (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to find details about a Domain Name System (DNS). Use this command from an ArcSight Console running Windows.
- **Ping (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to test whether a particular host is reachable across an IPv4 network. Use this command from an ArcSight Console running Linux.
- **Ping6 (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to test whether a particular host is reachable across an IPv6 network. Use this command from an ArcSight Console running Linux.
- **Ping (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to test whether a particular host is reachable across an IPv4 or IPv6 network. Use this command from an ArcSight Console running Windows.

- **Portinfo (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find information about the selected port. Use this command from an ArcSight Console running Linux.
- **Portinfo (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to find information about the selected port. Use this command from an ArcSight Console running Windows.
- **Traceroute (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Linux.
- **Traceroute (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Windows.
- **Web Search** enables you to run a search with the selected item, device vendor, and device product in the selected event.
- **Whois (Linux)** /All Integration Commands/ArcSight System/Tools/Linux enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Linux.
- **Whois (Windows)** /All Integration Commands/ArcSight System/Tools/Windows enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Windows.

Appendices

These appendices contain lists of resources available to you to help you monitor your environment.

- [ArcSight Administration Content](#)
- [Security Monitoring - Base - Active Lists Content](#)
- [Security Monitoring - Base Content](#)
- [Security Threat Monitoring Content](#)
- [Threat Intelligence Platform Content](#)

ArcSight Administration Content

This appendix contains tables of resources organized by resource for the ArcSight Administration package.

[Active Channels](#)

[Active Lists](#)

[Dashboards](#)

[Data Monitors](#)

[Field Sets](#)

[Fields](#)

[Filters](#)

[Integration Commands, Configuration, and Target](#)

[Queries](#)

[Query Viewers](#)

[Rules](#)

[Session Lists](#)

[Use Cases](#)

Active Channels

Name	Description	Location
Connector Upgrades	Displays all the events related to connector upgrades within the last two hours. The active channel uses the Connector Upgrades field set.	/All Active Channels/ArcSight Administration/Connectors/Configuration Changes/Connector Upgrades
Connector Connection Status Events	Displays information about connector connection-status audit events and correlation events from the related Connector Monitoring rules.	/All Active Channels/ArcSight Administration/Connectors/System Health/Connector Connection Status Events
Distributed Correlation Audit Events	Displays distributed correlation audit events.	/All Active Channels/ArcSight Administration/Detect/Distributed Correlation Monitoring/Distributed Correlation Audit Events
ASM Events	Displays ArcSight System Monitoring events generated by the local ArcSight Detect system.	/All Active Channels/ArcSight Administration/Detect/System Health/Events/ASM Events
Query Viewers Status	Displays all the query viewer-related events within the last two hours.	/All Active Channels/ArcSight Administration/Detect/System Health/Resources/Query Viewers Status
ArcSight Detect Device Monitoring	Displays device status events.	/All Active Channels/ArcSight Administration/Devices/ArcSight Detect Device Monitoring

Active Lists

Some active lists require configuration by the customer, these are marked with an asterisk.

Name	Description	Location
Connector Upgrades	Stores information related to successful and failed connector upgrades. When an upgrade is successful, the active list stores the Upgrade Time, Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. When an upgrade fails, the active list also stores the reason for the failure. The active list is populated by the Connector Upgrade Failed and Connector Upgrade Successful rules.	/All Active Lists/ArcSight Administration/Connectors/Configuration Changes/Connector Upgrades
Connector Information	Maintains a list of the available information about connectors, whether they are directly connected to an Detect manager or indirectly through a Logger. Note: Information is derived from connector audit events and some information might be incomplete (blank) until the appropriate audit event arrives and is processed by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/Connector Information
Connectors - Down	Stores the IDs and names of connectors that are currently down (either a connector shut down or a heartbeat timeout). After the TTL of the active list expires, the connector information is added to the Connectors Still Down active list and a notification is sent to the SOC Operators to inform them that the connector has been down for 20 or more minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/Connectors - Down
Connectors - Still Down	Stores the ID and the name of the connectors that are have been down for 20 minutes or more (either a connector shut down or a heartbeat timeout). After the TTL of the Connectors - Down active list expires, the connector information is added to this list and a notification is sent to the SOC Operators to inform them that the connector has been down for more than 20 minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/Connectors - Still Down
Black List - Connectors	Maintains a list of connectors that are not monitored by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/Black List - Connectors

Name	Description	Location
Black List - Reverse Look Up	<p>Stores look-up data to enable the rules to update the connector connection and caching status displays when a connector is added to the Black List - Connectors active list.</p> <p>Note: This list should contain all the information that is also included in the Connector Information active list. This active list links the information in the Black List - Connectors active list to the information in the Connector Information active list. The connectors listed in the Black List - Connectors active list are the only ones not processed by the Connector Monitoring rules. Do not edit the entries in this list unless you are sure that an entry is no longer valid (and can be removed).</p>	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/Black List - Reverse Look Up
Connector Average EPS - Last 7 Days	Stores the average EPS for all connectors during the last seven days. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/Connector Average EPS - Last 7 Days
Connector Daily Average EPS	Stores the daily average EPS for all connectors. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/Connector Daily Average EPS
Average EPS	Stores average EPS during last hour.	/All Active Lists/ArcSight Administration/Detect/Distributed Correlation Monitoring/Average EPS
Counts from Distributed Correlation	Stores hourly event counts for correlator and aggregator.	/All Active Lists/ArcSight Administration/Detect/Distributed Correlation Monitoring/Counts from Distributed Correlation
Counts in Persistor	Stores hourly event counts in persistor.	/All Active Lists/ArcSight Administration/Detect/Distributed Correlation Monitoring/Counts in Persistor
Storage Licensing Data by Connector	Stores the raw event length reported by the raw event statistics events for each connector.	/All Active Lists/ArcSight Administration/Detect/Licensing/Storage Licensing Data by Connector
Invalid Resources	Stores a list of resources that become invalid. The Resource Became Invalid rule adds an entry to the active list and the Resource Became Valid rule removes the corresponding entry from the active list.	/All Active Lists/ArcSight Administration/Detect/System Health/Resources/Invalid Resources
Query Running Time	Stores query information used to monitor and report the query duration.	/All Active Lists/ArcSight Administration/Detect/System Health/Resources/Query Running Time

Name	Description	Location
All Monitored Devices	Populated by the All Monitored Devices rule. The active list stores entries for 365 days and is used by queries to retrieve device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/All Monitored Devices
Critical Devices *	Populated manually and used by the Critical Monitored Devices rule first. If the rule finds a match, it updates the Critical Monitored Devices active list, which in turn is used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/Critical Devices
Critical Monitored Devices *	Populated manually at first and then updated by the Critical Monitored Devices rule. The entries in this active list never expire, and are used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/Critical Monitored Devices
Whitelisted Monitored Devices	Includes non-critical devices that you want to exclude from monitoring. This list is populated manually. The entries never expire.	/All Active Lists/ArcSight Administration/Devices/Whitelisted Monitored Devices

Dashboards

Name	Description	Location
Connector Connection Status	Displays the overall status of connectors and information on connectors that are down, caching, or dropping events.	/All Dashboards/ArcSight Administration/Connectors/System Health/Connector Connection Status
Current Event Sources	Displays information about the status of your connectors, as well as the top devices (vendor and product) that are contributing events.	/All Dashboards/ArcSight Administration/Connectors/System Health/Current Event Sources
Resource Change Log	Displays the changes (add, update, delete) to content resources and detailed information about logs associated with those actions.	/All Dashboards/ArcSight Administration/Detect/Configuration Changes/Resources/Resource Change Log
Event Overview	Displays an overview of non-ArcSight events focusing on Events Counts, Events by Connector, Events by Vendor and Product, and Events by Device Address.	/All Dashboards/ArcSight Administration/Detect/Event Analysis Overview/Event Overview
Detect System Information	Displays the System Information data monitor, which provides version, licensing, system resources availability and statistics, and other important settings and status.	/All Dashboards/ArcSight Administration/Detect/System Health/Detect System Information
Event Throughput	Displays the Event Throughput and Event Throughput Statistics data monitors, providing an overview of the system activity related to connectors.	/All Dashboards/ArcSight Administration/Detect/System Health/Events/Event Throughput

Name	Description	Location
Latest Events By Priority	Displays event count distribution ordered by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.	/All Dashboards/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority
Data Monitor Status	Displays the status of data monitors. Detailed information about event count, processing time, DCache Sync Count, DCache Sync Time are shown.	/All Dashboards/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Data Monitor Status
Query Running Time Overview	Displays the top ten longest queries for report, trend, and query viewers. The dashboard also shows query counts by type of queries.	/All Dashboards/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Running Time Overview
Query Viewer Details	Displays query details for query viewers.	/All Dashboards/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewer Details
Rules Status	Displays the status of the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, Sortable Rule Stats, and error logs are shown.	/All Dashboards/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status
ArcSight User Activity	Displays login session information and notification activity for ArcSight Detect users.	/All Dashboards/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Activity
ArcSight User Status	Displays the ArcSight User Sessions data monitor, showing recent login/logout activity for users, the remote terminal and zone, and current status.	/All Dashboards/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Status
All Monitored Devices	Displays an overview of all Detect devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	/All Dashboards/ArcSight Administration/Devices/All Monitored Devices
Critical Monitored Devices	Displays an overview of the critical devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	/All Dashboards/ArcSight Administration/Devices/Critical Monitored Devices

Data Monitors

Name	Description	Location
Connector Connection Status	Displays the current status of the connector connections across all connectors. If one or more connectors is down for less than 20 minutes (by default), the status is yellow (short-term outage). If one or more connectors is down for longer than 20 minutes, the status is red (long-term outage).	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Connection Status/Connector Connection Status
Current Connector Status	Displays information about the connectors that are registered with the system and reporting events.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/Current Connector Status
Top Event Sources	Displays the most common event generating products and displays a listing of the top 20.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/Top Event Sources
Recent System Resource Deletes	Displays deleted resources. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/Configuration Changes/Resources/Recent System Resource Deletes
Recent System Resource Inserts	Displays inserted resources. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/Configuration Changes/Resources/Recent System Resource Inserts
Recent System Resource Updates	Displays updated resources. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/Configuration Changes/Resources/Recent System Resource Updates
Resource Change Log	Displays the resource change log. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/Configuration Changes/Resources/Resource Change Log/Resource Change Log
Resource Change Overview	Displays the resource change overview. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/Configuration Changes/Resources/Resource Change Log/Resource Change Overview
Event Counts	Displays all non-ArcSight events.	/All Data Monitors/ArcSight Administration/Detect/Event Analysis Overview/Event Overview/Event Counts

Name	Description	Location
Events by Connector	Displays the total number of non-ArcSight events by connector.	/All Data Monitors/ArcSight Administration/Detect/Event Analysis Overview/Event Overview/Events by Connector
Events by Device Address	Displays all non-ArcSight events by device address.	/All Data Monitors/ArcSight Administration/Detect/Event Analysis Overview/Event Overview/Events by Device Address
Events by Vendor and Product	Displays all non-ArcSight events by vendor and product.	/All Data Monitors/ArcSight Administration/Detect/Event Analysis Overview/Event Overview/Events by Vendor and Product
System Information	Displays system information about this ArcSight Detect.	/All Data Monitors/ArcSight Administration/Detect/System Health/Detect System Information/System Information
Event Throughput	Displays the average EPS (events per second) for all the events within the last hour. The sampling interval is five minutes.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Event Throughput/Event Throughput
Event Throughput Statistics	Displays event throughput from various connectors sending events to this ArcSight Detect.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Event Throughput/Event Throughput Statistics
Events By Priority	Displays events by priority. This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Events By Priority
Latest Elevated Threat Events	Displays the list of critical devices that are currently down. A device is down if it has not reported for a certain period of time (30 minutes by default).	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Latest Elevated Threat Events
Latest Guarded Threat Events	Displays information about the latest threat events with a priority level of 3 or 4.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Latest Guarded Threat Events
Latest High Threat Events	Displays information about the latest threat events with a priority level of 7 or 8.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Latest High Threat Events

Name	Description	Location
Latest Low Threat Events	Displays information about the latest threat events with a priority level less than or equal to 2.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Latest Low Threat Events
Latest Severe Threat Events	Displays information about the latest threat events with a priority level greater than 8.	/All Data Monitors/ArcSight Administration/Detect/System Health/Events/Latest Events By Priority/Latest Severe Threat Events
Top Data Monitors by DCache Sync Count	Displays the top data monitors by DCache sync count.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Top Data Monitors by DCache Sync Count
Top Data Monitors by DCache Sync Time	Displays the top data monitors by DCache sync time.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Top Data Monitors by DCache Sync Time
Top Data Monitors by Event Count	Displays the top data monitors by event count.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Top Data Monitors by Event Count
Top Data Monitors by Event Processing Time	Displays the top data monitors by event processing time.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Top Data Monitors by Event Processing Time
Partial Matches per Rule	Displays event counts for partial rule matches.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status/Partial Matches per Rule
Recent Fired Rules	Displays information about the most recently fired rules.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status/Recent Fired Rules
Rule Audit Events	Displays the most recent errors received from the rules engine.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status/Rule Audit Events

Name	Description	Location
Sortable Rule Stats (only applies to compact mode)	<p>Displays statistics for rule performance, such as partial matches, matching events, correlation events, time to execute, and memory used by each rule. You can sort the information in each column by clicking the column title.</p> <p>Note: Lightweight rules do not use in-memory operations or data field aggregation, and do not generate correlation events. Therefore, Matching Events, Correlation Events, and Aggregation Sets are always zero for lightweight rules.</p>	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status/Sortable Rule Stats (only applies to compact mode)
Top Firing Rules	Displays information about the top firing rules.	/All Data Monitors/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Status/Top Firing Rules
ArcSight User Sessions	Displays the status of the ArcSight user sessions to the ArcSight Manager. The data monitor shows the username, the IP address of the machine from which the user is connecting, and the status of the connection. The status of the connection can be: Logged in, Logged out, or Login Timed Out.	/All Data Monitors/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Status/ArcSight User Sessions
Current Users Logged In	Displays information about the users currently logged into the ArcSight Detect system.	/All Data Monitors/ArcSight Administration/Detect/User Access/User Sessions/Console and ArcSight Web Status/Current Users Logged In
Notification Log	Displays notification activity generated by ArcSight Detect rules. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/User Access/User Sessions/Console and ArcSight Web Status/Notification Log
User Access Log	Displays recent user session data events. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/Detect/User Access/User Sessions/Console and ArcSight Web Status/User Access Log

Field Sets

Name	Description	Location
Connector Monitoring Events	Contains fields used to examine connector monitoring events, such as specific connector audit events and correlation events resulting from rules in the Connector Monitoring use cases.	/All Field Sets/ArcSight Administration/Connector/Connector Monitoring Events
Connector Upgrades	Used by the Connector Upgrades active channel. The selected fields are: Manager Receipt Time, End Time, Name, Device Event Category, Agent Name, Agent Version, Agent Address, and Agent Zone Name.	/All Field Sets/ArcSight Administration/Connector/Connector Upgrades
ASM Events	Contains fields of interest for monitoring ASM events.	/All Field Sets/ArcSight Administration/Detect/ASM Events
Distributed Correlation Events	This field sets is for distributed correlation monitoring.	/All Field Sets/ArcSight Administration/Detect/Distributed Correlation Monitoring/Distributed Correlation Events
Query Status	Displays detailed information about queries.	/All Field Sets/ArcSight Administration/Detect/Query Status
ArcSight Detect Device Monitoring	Contains fields used to examine device status events.	/All Field Sets/ArcSight Administration/Devices/ArcSight Detect Device Monitoring

Fields

All fields function as variables unless otherwise noted.

Name	Description	Location
AverageEPS	Returns 1000 if LastHourEPS is null.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/AverageEPS
EPS	Returns string EPS.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/EPS
getAddress	Returns the source address if it is not null, otherwise it returns the destination address.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/getAddress
getHourOfDay	Returns hour of manager receipt time.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/getHourOfDay

Name	Description	Location
getLastHour	Returns last hour of manager receipt time.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/getLastHour
LastHourEPS	Returns last hour average EPS in persistor.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/LastHourEPS
OneHourEvents	Returns one hour events based on last hour average EPS.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/OneHourEvents
TenMinutesEvents	Returns 10 minutes events based on last hour average EPS.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/TenMinutesEvents
ConnectorID	Returns the Resource ID of the connector.	/All Fields/ArcSight Administration/Detect/Licensing/ConnectorID
ConnectorName	Returns the name of the connector.	/All Fields/ArcSight Administration/Detect/Licensing/ConnectorName
ConnectorNameFromID	Returns the name of the connector by looking up the Connector ID in the Connector Information Active List.	/All Fields/ArcSight Administration/Detect/Licensing/ConnectorNameFromID
ConnectorType	Returns the type of connector.	/All Fields/ArcSight Administration/Detect/Licensing/ConnectorType

Filters

Name	Description	Location
Connector Caching Event	Detects connector caching events.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/Connector Caching Event
Connector Registered or Heartbeat Event	Detects events for connector timeouts because the connector information is not complete in Device Custom String2.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/Connector Registered or Heartbeat Event
Connector Connection Status	Detects correlation events related to connector connection status.	/All Filters/ArcSight Administration/Connectors/System Health/Connector Connection Status

Name	Description	Location
Resource Changes	Detects resource change audit events.	/All Filters/ArcSight Administration/Detect/Configuration Changes/Resource Update Tracking/Resource Changes
Resource Deletes	Detects deleted resources.	/All Filters/ArcSight Administration/Detect/Configuration Changes/Resource Update Tracking/Resource Deletes
Resource Inserts	Detects new resources.	/All Filters/ArcSight Administration/Detect/Configuration Changes/Resource Update Tracking/Resource Inserts
Resource Updates	Detects updates to resources.	/All Filters/ArcSight Administration/Detect/Configuration Changes/Resource Update Tracking/Resource Updates
Aggregator Audit Events	Detects audit events for aggregator.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Aggregator Audit Events
Correlator Audit Events	Detects audit events for correlator.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Correlator Audit Events
Distributed Cache Audit Events	Detects audit events for distributed cache.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Distributed Cache Audit Events
Distributed Correlation Audit Events	Detects audit events for distributed correlation.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Distributed Correlation Audit Events
Green Threshold	Detects event remaining count in message bus is less than certain time events, by default, it is 10 minutes.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Green Threshold
Message Bus Status Events	Detects status audit events for message bus.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Message Bus Status Events

Name	Description	Location
Message Count Remaining in Message Bus	Detects audit events for messages remaining in message bus.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Message Count Remaining in Message Bus
Red Threshold	Detects event remaining count in message bus exceeds certain time events, by default, it is one hour.	/All Filters/ArcSight Administration/Detect/Distributed Correlation Monitoring/Red Threshold
ArcSight Status Monitoring Events	Detects ArcSight Status Monitoring events generated by the local ArcSight Detect system.	/All Filters/ArcSight Administration/Detect/System Health/ArcSight Status Monitoring Events
ASM Load Overview	Detects events that identify the load associated with the ArcSight Detect system through various parameters such as CPU, database, flow levels, memory, and resources.	/All Filters/ArcSight Administration/Detect/System Health/ASM Load Overview
ASM Event Flow	Detects events that identify the Detect load through flow levels of events.	/All Filters/ArcSight Administration/Detect/System Health/Events/ASM Event Flow
ArcSight Audit Events	Detects ArcSight Detect audit events.	/All Filters/ArcSight Administration/Detect/System Health/Events/Audit/ArcSight Audit Events
Notification Actions	Detects events that are related to notifications generated by a rule in the ArcSight Detect system.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Flow/Notification Actions
Elevated Threat Condition	Detects events with a Priority level rating of 5 or 6.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Priority Filters/Elevated Threat Condition
Guarded Threat Condition	Detects events with a Priority level rating of 3 or 4.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Priority Filters/Guarded Threat Condition
High Threat Condition	Detects events with a Priority level rating of 7 or 8.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Priority Filters/High Threat Condition
Low Threat Condition	Detects events with a Priority level rating less than or equal to 2.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Priority Filters/Low Threat Condition

Name	Description	Location
Severe Threat Condition	Detects events with Priority level rating greater than 8.	/All Filters/ArcSight Administration/Detect/System Health/Events/Event Priority Filters/Severe Threat Condition
ASM CPU Load	Detects ArcSight Detect monitoring events related to CPU load.	/All Filters/ArcSight Administration/Detect/System Health/Resources/ASM CPU Load
ASM Event Evaluation	Detects ArcSight Detect events based on rule insert event rates, data monitor evaluations per second, and filter evaluation counts.	/All Filters/ArcSight Administration/Detect/System Health/Resources/ASM Event Evaluation
ASM Flow Load	Detects ArcSight Detect monitoring events related to event flow.	/All Filters/ArcSight Administration/Detect/System Health/Resources/ASM Flow Load
ASM Resource and Memory Load	Detects ArcSight Detect monitoring events related to resource and memory load.	/All Filters/ArcSight Administration/Detect/System Health/Resources/ASM Resource and Memory Load
ASM Standing Load	Detects currently active, data monitor, rules, and active channel related events.	/All Filters/ArcSight Administration/Detect/System Health/Resources/ASM Standing Load
ASM Asset Resolution Timings	Detects ArcSight Status Monitor events that contain asset resolution timing information. The asset resolution average time is the average time in milliseconds taken to resolve an end-point in an event to an asset.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Assets/ASM Asset Resolution Timings
ASM Total Asset Count	Detects ArcSight System Monitor events that contain the current total number of assets.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Assets/ASM Total Asset Count
Data Monitor DCache Sync Counts	Detects ArcSight Detect DCache sync counts telemetry events generated by data monitors.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Data Monitor DCache Sync Counts
Data Monitor Event Counts	Detects ArcSight Detect event count telemetry events generated by data monitors.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Data Monitors/Data Monitor Event Counts
ArcSight Rules	Detects ArcSight Detect correlation events generated by rules.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Rules/ArcSight Rules

Name	Description	Location
Rules Engine Internal Events	Detects internal ArcSight Detect rules engine base events.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Rules/Rules Engine Internal Events
Hour less than 10	This filter is used by a Conditional DV. The condition in the filter is Hour(EndTime) is less than 10.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Trends/Conditional Variable Filters/Hour less than 10
Minute less than 10	This filter is used by a Conditional DV. The condition in the filter is Minute(EndTime) is less than 10.	/All Filters/ArcSight Administration/Detect/System Health/Resources/Trends/Conditional Variable Filters/Minute less than 10
ASM Database Load Statistics	Detects events related to ArcSight Detect database load.	/All Filters/ArcSight Administration/Detect/System Health/Storage/ASM Database Load Statistics
ASM Database Statistics	Detects events related to ArcSight Detect database statistics (such as insertion/retrieval).	/All Filters/ArcSight Administration/Detect/System Health/Storage/ASM Database Statistics
ASM Sidetable Cache Hit Rates	Detects ArcSight System Monitor events that contain side table cache hit rate information. Side tables are tables held in memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The cache hit rate identifies how many successful attempts were made to find entries within the past two hours.	/All Filters/ArcSight Administration/Detect/System Health/Storage/ASM Sidetable Cache Hit Rates
ASM Sidetable Sizes	Detects ArcSight System Monitor events that contain side table size information. Side tables are tables held in memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The side table size identifies how many entries are currently in the cache.	/All Filters/ArcSight Administration/Detect/System Health/Storage/ASM Sidetable Sizes
Threshold - Critical	This filter is used in the ASM Database Free Space - Critical rule. The filter identifies events in which the free space is less than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/Detect/System Health/Storage/Custom/Threshold - Critical

Name	Description	Location
Threshold - Warning	This filter is used in the ASM Database Free Space - Warning rule. The filter captures events where the free space is less than or equal to five percent, but more than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/Detect/System Health/Storage/Custom/Threshold - Warning
Database Insert Time Statistics	Detects ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime.	/All Filters/ArcSight Administration/Detect/System Health/Storage/Database Insert Time Statistics
Database Retrieval Time Statistics	Detects ArcSight system events where the Device Event Category is /Monitor/EventBroker/RetrievalTime.	/All Filters/ArcSight Administration/Detect/System Health/Storage/Database Retrieval Time Statistics
ArcSight Login Events	Detects events that are associated with logins to the ArcSight Detect system.	/All Filters/ArcSight Administration/Detect/User Access/User Sessions/ArcSight Login Events
ArcSight Login Rule Firings	Detects events that contain ArcSight login rule triggering information. The deviceEventCategory used in this filter is generated by the ArcSight User Login rule. The filter is used by a trend that tracks hourly login statistics.	/All Filters/ArcSight Administration/Detect/User Access/User Sessions/ArcSight Login Rule Firings
ArcSight Login Tracking	Detects events that contain ArcSight login and logout information. The device event class IDs used in this filter are generated by the ArcSight auditing system.	/All Filters/ArcSight Administration/Detect/User Access/User Sessions/ArcSight Login Tracking

Integration Commands, Configuration, and Target

Name	Description	Location
By Source and Destination	This integration command enables you to run a search by source and destination address on an ArcSight Recon.	/All Integration Commands/ArcSight Administration/ArcSight Recon/By Source and Destination
By Vendor and Product	This integration command enables you to run a search by device vendor and product on an ArcSight Recon.	/All Integration Commands/ArcSight Administration/ArcSight Recon/By Vendor and Product

Name	Description	Location
ArcSight Recon Search	This integration configuration is used to configure the ArcSight Recon search commands.	/All Integration Configurations/ArcSight Administration/ArcSight Recon/ArcSight Recon Search
ArcSight Recon 1	This integration target stores the hostname and port number of an ArcSight Recon. This target is used by the set of integration commands for ArcSight Recon search.	/All Integration Targets/ArcSight Administration/ArcSight Recon/ArcSight Recon 1

Queries

Queries have individual tables organized by sub-folder.

Connectors

Name	Description	Location
Connector Upgrades Count	Retrieves the count of successful and failed connector upgrades per day in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Connector Upgrades Count
Connector Upgrades Count (Total)	Retrieves the total count of successful and failed connector upgrades in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Connector Upgrades Count (Total)
Failed Connector Upgrades	Retrieves the connectors with failed upgrades (and the reason for the failure) in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Failed Connector Upgrades
Successful Connector Upgrades	Retrieves the connectors with successful upgrades (and the new connector version) in the Connectors Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Successful Connector Upgrades
Upgrade History by Connector	Retrieves all the connector upgrades (successful and failed) by connector in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Upgrade History by Connector
Upgrade History by Connector Type	Retrieves all the connector upgrades (successful and failed) by connector type in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/Upgrade History by Connector Type
Connector Versions	Retrieves all the connectors with their latest versions in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/Connector Versions

Name	Description	Location
Connector Versions by Type	Retrieves all the connectors with their latest versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/Connector Versions by Type
Version History by Connector	Retrieves all the connector versions by connector in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/Version History by Connector
Version History by Connector Type	Retrieves all the connectors and connector versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/Version History by Connector Type
Connectors - Down	Retrieves data on connectors that have been down for under 20 minutes (by default). The queries are used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/Connectors - Down
Connectors - Still Down	Retrieves data on connectors that have been down for longer than 20 minutes (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/Connectors - Still Down

Detect

Name	Description	Location
EPS Received in Correlator	Retrieves EPS count for events received in correlator.	/All Queries/ArcSight Administration/Detect/Distributed Correlation Monitoring/EPS Received in Correlator
Hourly EPS in Persistor	Retrieves hourly EPS in persistor.	/All Queries/ArcSight Administration/Detect/Distributed Correlation Monitoring/Hourly EPS in Persistor
MPS Received in Aggregator	Retrieves messages per second (MPS) count for events received in aggregator.	/All Queries/ArcSight Administration/Detect/Distributed Correlation Monitoring/MPS Received in Aggregator
Licensing Query	Retrieves the licensing history for the various license types taken from the License History session list.	/All Queries/ArcSight Administration/Detect/Licensing/Licensing Query
Storage Licensing Data	Retrieves the raw event length for each day for all the connectors from an active list.	/All Queries/ArcSight Administration/Detect/Licensing/Storage Licensing Data
Invalid Resources	Retrieves a list of invalid resources from the Invalid Resources active list.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Invalid Resources

Name	Description	Location
Invalid Resources (Chart)	Retrieves the count of invalid resources by resource type from the Invalid Resources active list.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Invalid Resources (Chart)
Failed Queries	Retrieves failed queries for reports, trends, and query viewers. The query is used to build a trend and a query viewer.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Queries/Failed Queries
Query Counts During Last 24 hr	Retrieves the resource type and its counts from the Query Running Time active list.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Queries/Query Counts During Last 24 hr
Query Counts During Last Week	Retrieves resource types and their counts from the Query Running Time active list.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Queries/Query Counts During Last Week
Last 10 Query Viewer Queries	Retrieves query duration information for query viewers, ordered by end time.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Last 10 Query Viewer Queries
Longest Query Viewer Queries	Retrieves query duration information for query viewers, ordered by duration.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Longest Query Viewer Queries
Query Viewer Failures	Retrieves query duration information for failed query viewers.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Query Viewer Failures
Query Viewer Queries	Retrieves query duration information for query viewers used to build a trend.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Query Viewer Queries

Devices

Name	Description	Location
All Devices Detected Inactive - Last 24 Hours	Retrieves devices detected as inactive within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Devices Detected Inactive - Last 24 Hours
All Devices Detected Inactive - Last 7 Days	Retrieves devices detected as inactive within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Devices Detected Inactive - Last 7 Days

Name	Description	Location
All Monitored Devices	Retrieves devices from the All Monitored Devices active list.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices
All Monitored Devices - Green	Retrieves devices detected as active within the last 20 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Green
All Monitored Devices - Green Counter	Retrieves devices detected as active within the last 20 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Green Counter
All Monitored Devices - Red	Retrieves devices detected as inactive for more than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Red
All Monitored Devices - Red Counter	Retrieves devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Red Counter
All Monitored Devices - Yellow	Retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Yellow
All Monitored Devices - Yellow Counter	Retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices - Yellow Counter
New Devices Detected - Last 24 Hours	Retrieves all new devices detected within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/New Devices Detected - Last 24 Hours
New Devices Detected - Last 7 Days	Retrieves all new devices detected within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/New Devices Detected - Last 7 Days
Critical Devices Detected Inactive - Last 24 Hours	Retrieves critical devices detected as inactive within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Devices Detected Inactive - Last 24 Hours
Critical Devices Detected Inactive - Last 7 Days	Retrieves critical devices detected as inactive within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Devices Detected Inactive - Last 7 Days

Name	Description	Location
Critical Monitored Devices	Retrieves critical devices from the Critical Monitored Devices active list.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices
Critical Monitored Devices - Green	Retrieves critical devices detected as active within the last 20 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Green
Critical Monitored Devices - Green Counter	Retrieves critical devices detected as active within the last 20 minutes and sorts them by product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Green Counter
Critical Monitored Devices - Red	Retrieves critical devices detected as inactive for more than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Red
Critical Monitored Devices - Red Counter	Retrieves critical devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Red Counter
Critical Monitored Devices - Yellow	Retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Yellow
Critical Monitored Devices - Yellow Counter	Retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices - Yellow Counter

Query Viewers

Name	Description	Location
Connectors - Down - Long Term	Displays data on connectors that have been down for longer than 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/Connectors - Down - Long Term
Connectors - Down - Short Term	Displays data on connectors that have been down for under 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/Connectors - Down - Short Term

Name	Description	Location
Hourly EPS Received in Correlator	Displays hourly EPS received in correlator.	/All Query Viewers/ArcSight Administration/Detect/Distributed Correlation Monitoring/Hourly EPS Received in Correlator
Hourly Messages Per Second Received in Aggregator	Displays hourly messages per second received in aggregator.	/All Query Viewers/ArcSight Administration/Detect/Distributed Correlation Monitoring/Hourly Messages Per Second Received in Aggregator
Query Counts During Last 24 hr	Displays the query and its counts during the last 24 hours.	/All Query Viewers/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Counts During Last 24 hr
Query Failures During Last 24 hr	Displays failed queries for reports, trends, and query viewers.	/All Query Viewers/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Failures During Last 24 hr
Last 10 Query Viewer Queries	Displays the last ten query viewer query duration information.	/All Query Viewers/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Last 10 Query Viewer Queries
Query Viewer Failures During Last 24 hr	Displays the failed query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Query Viewer Failures During Last 24 hr
Top 10 Longest Query Viewer Queries During Last 24 hr	Displays the duration information for the top ten longest query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Top 10 Longest Query Viewer Queries During Last 24 hr
Active Devices - last 20 min	Displays details for the devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Active Devices - last 20 min
Active Devices by Product - last 20 min	Displays details for the devices detected as active within the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Active Devices by Product - last 20 min

Name	Description	Location
All Monitored Devices	Displays details for the devices detected within the last 365 days.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/All Monitored Devices
Inactive Devices - more than 20 min	Displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Inactive Devices - more than 20 min
Inactive Devices - more than 60 min	Displays details for the devices detected as inactive for more than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Inactive Devices - more than 60 min
Inactive Devices by Product - more than 20 min	Displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Inactive Devices by Product - more than 20 min
Inactive Devices by Product - more than 60 min	Displays details for the devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - All/Inactive Devices by Product - more than 60 min
Active Critical Devices - last 20 min	Displays details for the critical devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Active Critical Devices - last 20 min
Active Critical Devices by Product - last 20 min	Displays details for the critical devices detected as active for the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Active Critical Devices by Product - last 20 min
Critical Monitored Devices	Displays details for all critical devices.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Critical Monitored Devices
Inactive Critical Devices - more than 20 min	Displays This query viewer displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Inactive Critical Devices - more than 20 min

Name	Description	Location
Inactive Critical Devices - more than 60 min	Displays details for the critical devices detected as inactive for more than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Inactive Critical Devices - more than 60 min
Inactive Critical Devices by Product - more than 20 min	Displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Inactive Critical Devices by Product - more than 20 min
Inactive Critical Devices by Product - more than 60 min	Displays details for the critical devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight Detect Device Monitoring - Critical/Inactive Critical Devices by Product - more than 60 min

Rules

Rules have individual tables organized by sub folder.

Connectors

Name	Description	Location
Connector Deleted	Detects connector deleted events that are sent when a connector is deleted from the resource tree. On the first event, the session for the corresponding connector is terminated in the Connector Versions session list, and the connector is also removed from the Connectors - Down active list.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/Configuration Changes/Connector Deleted
Connector Upgrade Failed	Detects failed connector upgrades. On every event, the connector information is added to the Connector Upgrades active list.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/Configuration Changes/Connector Upgrade Failed
Connector Upgrade Successful	Detects successful connector upgrades. On every event, the connector information is added to the Connector Upgrades active list. A new session is created in the Connector Versions session list. Note: The Agent configuration updated events are removed to avoid duplicate entries in the active list and session list.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/Configuration Changes/Connector Upgrade Successful

Name	Description	Location
Connector Version Detected	Detects connector start events. The rule triggers if the connector is not yet in the Connector Versions session list. On every event, a new session with the connector information is created in the Connector Versions session list.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/Configuration Changes/Connector Version Detected
Connector Discovered or Updated	Detects new connectors reporting to Detect and adds them to active lists to be monitored. Device Event Class ID = agent:007 is related to Agent Registration events. Device Event Class ID = agent:030 is related to Agent Start events. Device Event Class ID = agent:031 is related to Agent Shutdown events. Device Event Class ID = agent:101 is related to Agent Connection events. Device Event Class ID = agent:103 is related to Agent Heartbeat Timeout events. Device Event Class ID = agent:051 is related to Agent Failover events. These events contain the detailed information necessary to populate the Connectors active lists.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Connector Discovered or Updated
Connector Down	Detects connector shutdowns or heartbeat timeout events (except for connectors listed in the Black List - Connectors filter). The rule adds connector information to the Connectors - Down active list.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Connector Down
Connector Still Down	Detects when the TTL (20 minutes by default) for an entry in the Connectors - Down active list expires. The rule then adds the connector information to the Connectors - Still Down active list, creates a case and sends a notification to SOC Operators. Note: The case creation and notification actions are disabled by default.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Connector Still Down
Connector Up	Detects connector started events (except for connectors that match the conditions in the Black List - Connectors filter). The rule removes the connector from the connector connection status active lists.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Connector Up
Connector Added to Black List	Monitors the Black List - Connectors active list for new connector information. When a connector is added to the black list, this rule updates the other Connector Monitoring active lists to remove that connector from the status displays.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Custom/Connector Added to Black List
Update Connector Connection Status	Monitors audit events for changes in the connector connection status active lists. The rule then sets the device custom number and the string information used by the Connector Connection Status data monitor.	/All Rules/Real-time Rules/ArcSight Administration/Connectors/System Health/Update Connector Connection Status

Detect

Name	Description	Location
Detect Event Counts for Persistor	Populates the event counts for distributed correlation to a list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/Distributed Correlation Monitoring/Detect Event Counts for Persistor
Detect Events for Distributed Correlation	Populates the event counts for distributed correlation to a list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/Distributed Correlation Monitoring/Detect Events for Distributed Correlation
License Audit Event Detected	Detects when a license audit event is detected. The rule adds the license type, the current count, and the count limit to the License History session list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/Licensing/License Audit Event Detected
Storage Licensing Audit event Detected	Detects connector raw-event-statistic events and stores them in an active list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/Licensing/Storage Licensing Audit event Detected
Out of Domain Fields	Detects when there is no more free domain field available for a field type.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Domains/Out of Domain Fields
Invalid Resource Deleted	Detects Removes an invalid resource from the Invalid Resources active list when that resource is deleted. The rule triggers only if the resource that has been deleted is in the Invalid Resources active list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Invalid Resource Deleted
Query Running Time	Detects when a query audit event is detected. The rule adds or updates the corresponding entry in the active list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Query Running Time
Resource Became Invalid	Detects when a resource becomes invalid. The rule adds the resource ID, name, URI, and type to the Invalid Resources active list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Resource Became Invalid
Resource Became Valid	Detects when an invalid resource becomes valid. The rule removes the resource from the Invalid Resources active list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Resource Became Valid
Excessive Rule Recursion	Detects excessive rule recursion. This rule looks for events coming from the ArcSight Security Manager with the Device Event Category set to /Rule/Warning/Loop. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Rules/Excessive Rule Recursion

Name	Description	Location
Rule Matching Too Many Events	Detects rules that match too many events. The rule identifies events that come from the ArcSight Security Manager with the Device Event Category set to /Rule/Error/Deactivate/Unsafe. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Rules/Rule Matching Too Many Events
Warning - System Resources Exhausted	Indicates that a device has detected a system resource issue. The rule triggers whenever a resource is exhausted or a resource check fails. On the first event, a notification is sent to SOC operators. Note: This rule does not produce completely accurate results when running in Turbo Mode Fastest.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Resources/Warning - System Resources Exhausted
ASM Database Free Space - Critical	Detects internal events showing that one (or more) of the ASM database table spaces has a very low free space percentage. This is considered critical when the free space goes below the threshold defined in the server.properties file (two percent by default). A notification is sent to the Database Storage Operator group.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Free Space - Critical
ASM Database Free Space - Warning	Detects internal events showing that one (or more) of the ASM database table spaces has a low free space percentage. This is considered a warning when the free space goes below the threshold defined in the server.properties file (five percent by default).	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Free Space - Warning
ASM Database Status Change - Critical	Detects critical database status. This rule detects the insert and retrieval time for an event; the status is considered critical when the EventInsertTimeNanos field is greater than or equal to 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to very high.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Critical
ASM Database Status Change - Down	Detects down database status. This rule detects the insert and retrieval time for an event; the status is considered down when the EventInsertTimeNanos field is equal to zero. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to unknown.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Down
ASM Database Status Change - Normal	Detects normal database status. This rule detects the insert and retrieval time of the event; the status is considered normal when the EventInsertTimeNanos (insert time in nanoseconds) field is less than or equal to 20,000. This rule requires two such events within two minutes. After the first event, the agentSeverity event field is set to low.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Normal

Name	Description	Location
ASM Database Status Change - Space Critical	Detects critical database status due to storage concerns. This rule detects a base event indicating that the database storage space is low. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to very high.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Space Critical
ASM Database Status Change - Space Now Available	Detects if the database status has returned to normal because storage space has been freed or added. This rule detects a base event indicating that database storage space is available. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to Low.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Space Now Available
ASM Database Status Change - Warning	Detects warning level database status. This rule detects the insert and retrieval time for an event; the status is considered a warning when the EventInsertTimeNanos field is between 20,000 and 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to medium.	/All Rules/Real-time Rules/ArcSight Administration/Detect/System Health/Storage/ASM Database Status Change - Warning
ArcSight User Login	Detects ArcSight user login events. This rule adds the user information to the ArcSight User Sessions session list.	/All Rules/Real-time Rules/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Login
ArcSight User Login Timeout	Detects ArcSight user login timeout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user login timeout occurs.	/All Rules/Real-time Rules/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Login Timeout
ArcSight User Logout	Detects ArcSight user logout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user logout occurs.	/All Rules/Real-time Rules/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Logout

Devices

Name	Description	Location
Alert - Critical Devices inactive for more than 1 hour	Detects when a Connector Device Status event for critical devices has a zero in Device Custom Number2 and a Device Custom Date earlier than 60 minutes ago, which indicates that the device has been inactive for more than one hour. After the rule triggers, a notification is sent to the Device Administrators.	/All Rules/Real-time Rules/ArcSight Administration/Devices/Alert - Critical Devices inactive for more than 1 hour
All Monitored Devices	Detects when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check). After the rule triggers, the entry is created or updated in the All Monitored Devices active list.	/All Rules/Real-time Rules/ArcSight Administration/Devices/All Monitored Devices
Critical Monitored Devices	Detects when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check) and if the device entry exists in the Critical Monitored Devices active list. After the rule triggers, the active list entry is updated.	/All Rules/Real-time Rules/ArcSight Administration/Devices/Critical Monitored Devices

Session Lists

Name	Description	Location
Connector Versions	Stores the version history for all the connectors. The fields in the session list are: Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. The session list is populated by the Connector Upgrade Successful and Connector Version Detected rules.	/All Session Lists/ArcSight Administration/Connectors/Configuration Changes/Connector Versions
Licensing History	Stores the licensing history for the various license types. The session list stores the license type, the current count, and the count limit.	/All Session Lists/ArcSight Administration/Detect/Licensing/Licensing History
ArcSight User Sessions	Stores the client username, client address and zone used by an ArcSight user to access the ArcSight Manager to monitor the login times, logout times, or Console timeouts and to determine who had access to the system over specific time periods.	/All Session Lists/ArcSight Administration/Detect/User Access/User Sessions/ArcSight User Sessions

Use Cases

Name	Description	Location
Connector Overview	Covers administration content for monitoring connectors and devices.	/All Use Cases/ArcSight Administration/Connector Overview
Connector Configuration Changes	Provides information about configuration changes (such as upgrades) and connector version changes on the system.	/All Use Cases/ArcSight Administration/Connectors/Connector Configuration Changes
Connector Connection Status	Provides information about the connection status and caching status of connectors in the system. Connectors can be connected directly to Detect or through Loggers.	/All Use Cases/ArcSight Administration/Connectors/Connector Connection Status
Device Monitoring	Provides information about the devices reporting to Detect.	/All Use Cases/ArcSight Administration/Connectors/Device Monitoring
Detect Overview	Provides information about administration content for monitoring Detect.	/All Use Cases/ArcSight Administration/Detect Overview
Detect Resource Configuration Changes	Provides information about changes to the Detect resources, such as rules, reports, and so on.	/All Use Cases/ArcSight Administration/Detect/Configuration Changes/Detect Resource Configuration Changes
Detect Licensing	Provides information about Detect licensing compliance.	/All Use Cases/ArcSight Administration/Detect/Detect Licensing
Detect User Sessions	Provides information about user access to Detect.	/All Use Cases/ArcSight Administration/Detect/Detect User Sessions
Detect Events	Provides statistics about the flow of events through Detect.	/All Use Cases/ArcSight Administration/Detect/System Health/Detect Events
Detect Reporting Resource Monitoring	Provides information about performance statistics for reports, trends, and query viewers.	/All Use Cases/ArcSight Administration/Detect/System Health/Detect Reporting Resource Monitoring
Detect Resource Monitoring	Provides processing statistics for various Detect resources, such as trends, rules, and so on.	/All Use Cases/ArcSight Administration/Detect/System Health/Detect Resource Monitoring
ArcSight Detect Device Monitoring	Monitors the status of ArcSight Detect devices using the Device Status Monitoring (DSM) functionality that comes with SmartConnectors.	/All Use Cases/ArcSight Administration/Devices/ArcSight Detect Device Monitoring

Security Monitoring - Base - Active Lists Content

This appendix contains tables of resources organized by resource for the Security Monitoring - Base - Active Lists package.

- [Rules](#)
- [Active Lists](#)

Rules

Name	Description	Locations
Track Rules with MITRE ID	Tracks correlation events with device custom string 6 label is MITRE ID.	/All Rules/Real-time Rules/Track Rules with MITRE ID
Track Rules triggered	Tracks correlation events with device custom string 6 label is MITRE ID, and rules under threat intelligence platform group.	/All Rules/Real-time Rules/Track Rules triggered

Active Lists

Some active lists require configuration by the customer, these are marked with an asterisk.

Name	Description	Locations
Application List	Contains (suspicious) applications.	/All Active Lists/ArcSight Foundation/Common/Application List
Category for Exploit	Stores categories for exploit.	/All Active Lists/ArcSight Foundation/Common/Category for Exploit
Cleartext Protocols	Contains Cleartext Protocols.	/All Active Lists/ArcSight Foundation/Common/Cleartext Protocols
Commonly Used Ports	Contains the list of uncommonly used ports.	/All Active Lists/ArcSight Foundation/Common/Commonly Used Ports
Default Accounts*	Populate with the default accounts. Entries in this list should be in all capital case if it is not case sensitive.	/All Active Lists/ArcSight Foundation/Common/Default Accounts

Name	Description	Locations
Destination Process List	Contains a windows-known list of file names. Adversaries may use these files for masquerading techniques.	/All Active Lists/ArcSight Foundation/Common/Destination Process List
Indicator Types	This list syncs with Suspicious Indicator Types, which is maintained by two lightweight rules.	/All Active Lists/ArcSight Foundation/Common/Indicator Types
Interzone Communications to Restricted Services	Contains restricted services.	/All Active Lists/ArcSight Foundation/Common/Interzone Communications to Restricted Services
MITRE ATT&CK List	Contains Mitre Att&ck information.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK List
Privilege User Account	Populate with the usernames that have administrative privileges in your domain. Entries in this list should be in all capital case if it is not case sensitive.	/All Active Lists/ArcSight Foundation/Common/Privilege User Account
Privilege User Groups*	Populate with the user groups that have administrative privileges in your domain. Entries in this list should in capital case according to those formats: domain\group example EMEA\ADMINS builtin\group example BUILTIN\ADMINISTRATORS	/All Active Lists/ArcSight Foundation/Common/Privilege User Groups
Ransomware Notes	Contains known ransomware instruction filenames.	/All Active Lists/ArcSight Foundation/Common/Ransomware Notes
Suspicious Countries	Contains suspicious countries, for example itar prohibited countries.	/All Active Lists/ArcSight Foundation/Common/Suspicious Countries
Suspicious Indicator Types	Contains indicator types which can trigger certain rules.	/All Active Lists/ArcSight Foundation/Common/Suspicious Indicator Types
Suspicious Processes Launched From Microsoft Office Applications	Contains the list of processes that regularly do not have Microsoft Office applications as parent processes.	/All Active Lists/ArcSight Foundation/Common/Suspicious Processes Launched From Microsoft Office Applications

Name	Description	Locations
Threat Level Mapping	Maps the threat level to the severity and priority.	/All Active Lists/ArcSight Foundation/Common/Threat Level Mapping
Uncommonly Used Ports	Contains the list of uncommonly used ports.	/All Active Lists/ArcSight Foundation/Common/Uncommonly Used Ports
Windows Child Parent Process Relationship	Tracks child-parent Windows process normal relationships.	/All Active Lists/ArcSight Foundation/Common/Windows Child Parent Process Relationship

Security Monitoring - Base Content

This appendix contains tables of resources organized by resource for the Security Monitoring - Base package.

[Active Channel](#)

[Active Lists](#)

[Dashboards](#)

[Data Monitors](#)

[Field Set](#)

[Fields](#)

[Filters](#)

[Integration Command and Configuration](#)

[Queries](#)

[Query Viewers](#)

[Reports](#)

[Use Case](#)

Active Channel

Name	Description	Location
MITRE ATT&CK	Displays all correlation rules with Mitre Att&ck information.	/All Active Channels/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK

Active Lists

Some active lists require configuration by the customer, these are marked with an asterisk.

Name	Description	Location
External Device Connected With Autorun	Tracks external drives connected to machines having autorun.inf.	/All Active Lists/ArcSight Foundation/Common/External Device Connected With Autorun
Attacker and Target and Username Based Suppression	Suppression list based on attacker address, target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Attacker and Target and Username Based Suppression
Attacker and Target Based Suppression	Suppression list based on attacker address, target address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Attacker and Target Based Suppression
Attacker Based Suppression	Suppression list based on attacker address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Attacker Based Suppression
Host Name Based Suppression	Suppression list based on device host name and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Host Name Based Suppression
Host Name Based Suppression for Joined Rule	Suppression list based on hostname for joined rule.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Host Name Based Suppression for Joined Rule
Target and Username Based Suppression	Suppression list based on target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Target and Username Based Suppression
Target Based Suppression	Suppression list based on target address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Target Based Suppression
Username Based Suppression	Suppression list based on target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/Username Based Suppression

Name	Description	Location
Suspicious Activities Tracking	Tracks suspicious activities.	/All Active Lists/ArcSight Foundation/Common/Suspicious Activities Tracking
Terminated User Account	Stores terminated user accounts by username. If the username is not available, the user id can be added to this list. This list has to be populated manually in uppercase. Since domain is the key field, devices that do not report the domain should leave domain field blank.	/All Active Lists/ArcSight Foundation/Common/Terminated User Account
Track Rules Triggered	Tracks all triggered rules.	/All Active Lists/ArcSight Foundation/Common/Track Rules Triggered
MITRE ATT&CK Activity Tracking	Tracks MITRE ATT&CK Activity.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Activity Tracking
Rules Triggered with Mitre ID	Stores Mitre Att&ck information from correlation rules.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/Rules Triggered with Mitre ID

Dashboards

Name	Description	Location
MITRE Alerts Graph View	Displays MITRE alerts graph view.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE Alerts Graph View
MITRE ATT&CK Overview	Displays MITRE ATT&CK overview.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Overview
MITRE ATT&CK Targets Overview	Displays an overview of MITRE ATT&CK events with targets information.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Targets Overview

Data Monitors

Name	Description	Location
Last MITRE ATT&CK Events	Displays the last 5 MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Last MITRE ATT&CK Events
MITRE Alert Graph View	Displays MITRE alert graph view.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Alert Graph View

Name	Description	Location
MITRE Attackers and Targets Relations	Displays relationship between attacker and target machines using MITRE IDs. /All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Attackers and Targets Relations	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Attackers and Targets Relations
Top Fired MITRE ATT&CK Rules	Displays the top 5 fired rules with MITRE ATT&CK information.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Fired MITRE ATT&CK Rules
Top Target IPs	Displays the top 5 target IP addresses with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Target IPs
Top Target Users	Displays the top 5 users with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/Top Target Users

Field Set

Name	Description	Location
MITRE ATT&CK	Selects fields related Mitre Att&ck.	/All Field Sets/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK

Fields

Fields have been organized by sub-folder. All fields function as variables unless otherwise noted.

Common

Name	Description	Location
dc_agentHostname	Returns agent hostname.	/All Fields/ArcSight Foundation/Common/dc_agentHostname
dc_atkDnsDomain	Returns attacker DNS domain in lowercase.	/All Fields/ArcSight Foundation/Common/dc_atkDnsDomain
dc_atkHostName	Returns attacker host name in lowercase.	/All Fields/ArcSight Foundation/Common/dc_atkHostName
dc_atkProcessName	Returns process names from the attacker process name field and converts them to lower case.	/All Fields/ArcSight Foundation/Common/dc_atkProcessName

Name	Description	Location
dc_atkUserID	Returns attacker user IDs in uppercase.	/All Fields/ArcSight Foundation/Common/dc_atkUserID
dc_atkUserName	Returns attacker user names in uppercase.	/All Fields/ArcSight Foundation/Common/dc_atkUserName
dc_dstDnsDomain	Returns destination DNS domains in lowercase.	/All Fields/ArcSight Foundation/Common/dc_dstDnsDomain
dc_dstHostName	Returns destination hostnames in lowercase.	/All Fields/ArcSight Foundation/Common/dc_dstHostName
dc_dstUserName	Returns destination usernames in uppercase.	/All Fields/ArcSight Foundation/Common/dc_dstUserName
dc_dvcHostName	Returns device hostnames in lowercase.	/All Fields/ArcSight Foundation/Common/dc_dvcHostName
dc_endTimeinHour	Returns hour of end times.	/All Fields/ArcSight Foundation/Common/dc_endTimeinHour
dc_nullString	Returns null strings.	/All Fields/ArcSight Foundation/Common/dc_nullString
dc_serverHostName	Returns server host names.	/All Fields/ArcSight Foundation/Common/dc_serverHostName
dc_srcDnsDomain	Returns source DNS domains in lowercase.	/All Fields/ArcSight Foundation/Common/dc_srcDnsDomain
dc_srcHostName	Returns source hostnames in lowercase.	/All Fields/ArcSight Foundation/Common/dc_srcHostName
dc_srcUserName	Returns source usernames in uppercase.	/All Fields/ArcSight Foundation/Common/dc_srcUserName
dc_tgtDnsDomain	Returns target DNS domains in lowercase.	/All Fields/ArcSight Foundation/Common/dc_tgtDnsDomain
dc_tgtHostName	Returns target hostnames in lowercase.	/All Fields/ArcSight Foundation/Common/dc_tgtHostName
dc_tgtProcessName	Returns process names from target process name field and converts them to lower case.	/All Fields/ArcSight Foundation/Common/dc_tgtProcessName
dc_tgtUserID	Returns target user IDs in uppercase.	/All Fields/ArcSight Foundation/Common/dc_tgtUserID
dc_tgtUserName	Returns target usernames in uppercase.	/All Fields/ArcSight Foundation/Common/dc_tgtUserName
dc_userName	Returns the destination user name if it is not null. Otherwise, it returns the source user name.	/All Fields/ArcSight Foundation/Common/dc_userName

Name	Description	Location
linuxHostName	Global variable that gets information about the event generator from Linux events. It first tries to get the destination hostname from the event. If this is not shown in the event, it then tries to get the device hostname. If none of these is available, it gets the agent hostname.	/All Fields/ArcSight Foundation/Common/linuxHostName
dc_tgtAddress (tgtAddressByDirection)	Returns the destination addresses for outbound traffic and the source addresses for inbound traffic.	/All Fields/ArcSight Foundation/Common/Originator by Traffic Direction/dc_tgtAddress
dc_tgtAddressZone (tgtZoneByDirection)	Returns the destination zones for inbound traffic and the source zones for outbound traffic.	/All Fields/ArcSight Foundation/Common/Originator by Traffic Direction/atkZoneByDirection/dc_tgtAddressZone
dc_getOriginator (getOriginator)	Returns the string destinations for outbound traffic and the string sources for inbound traffic.	/All Fields/ArcSight Foundation/Common/Originator by Traffic Direction/dc_getOriginator
dc_atkAddress (atkAddressByDirection)	Returns the destination addresses for outbound traffic and the source addresses for inbound traffic.	/All Fields/ArcSight Foundation/Common/Originator by Traffic Direction/dc_atkAddress
dc_atkAddressZone (atkZoneByDirection)	Returns the destination zones for inbound traffic and the source zones for outbound traffic.	/All Fields/ArcSight Foundation/Common/Originator by Traffic Direction/dc_atkAddressZone
serverAddress	Returns server addresses.	/All Fields/ArcSight Foundation/Common/serverAddress
serverAddressZone	Returns server zones.	/All Fields/ArcSight Foundation/Common/serverAddressZone

MITRE ATT&CK

Name	Description	Location
getMitre	Returns Mitre ATT&CK information.	/All Fields/ArcSight Foundation/MITRE ATT&CK/getMitre
getTacticTriggeredRule	Converts tactics from lists to strings.	/All Fields/ArcSight Foundation/MITRE ATT&CK/getTacticTriggeredRule
getTriggeredRule	Returns detailed information of the triggered rule.	/All Fields/ArcSight Foundation/MITRE ATT&CK/getTriggeredRule

Name	Description	Location
mitreID	Converts MITRE IDs from lists to strings.	/All Fields/ArcSight Foundation/MITRE ATT&CK/mitreID
mitreName	Converts MITRE names from lists to strings.	/All Fields/ArcSight Foundation/MITRE ATT&CK/mitreName
taticName	Converts MITRE tactics from lists to strings.	/All Fields/ArcSight Foundation/MITRE ATT&CK/taticName

Filters

Name	Description	Location
After Work Hour	Identifies events occurring outside of working hours. The default is 7 a.m. to 7 p.m.	/All Filters/ArcSight Foundation/Common/Shared filters/After Work Hour
Attacker Host or Address Present	Identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Foundation/Common/Shared filters/Attacker Host or Address Present
Target Host or Address Present	Identifies events that have either the Target Host Name or Target Address event fields populated.	/All Filters/ArcSight Foundation/Common/Shared filters/Target Host or Address Present
Microsoft Windows Security Events	Contains the conditions for Windows security events.	/All Filters/ArcSight Foundation/Common/Shared filters/Windows/Microsoft Windows Security Events
MITRE Alerts	Selects MITRE alerts.	/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE Alerts
MITRE ATT&CK	Selects events with Mitre Att&ck information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK
MITRE ATT&CK with Attacker and Target	Selects events with Mitre Att&ck information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK with Attacker and Target

Name	Description	Location
Windows Events with a Non-Machine User	Identifies Microsoft Windows events that have a non machine/system users either in the attacker or the target fields.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/Windows Events with a Non-Machine User
Windows User Account Successful Logon	Contains the conditions for successful login of a Windows user account.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/Windows User Account Successful Logon
Categorization of Commonly used Keystroke Applications	Contains the categorization of commonly used Keystroke Applications.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Categorization of Commonly used Keystroke Applications

Integration Command and Configuration

Name	Description	Location
MITRE ATT&CK Lookup	Integration command used to look for MITRE ATT&CK technique details.	/All Integration Commands/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Lookup
MITRE ATT&CK Lookup	Integration configuration used to configure the MITRE ATT&CK lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configuration/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK Lookup

Queries

Name	Description	Location
Alert with Mitre ID Details	Selects details of an alert with MITRE Id.	/All Queries/ArcSight Foundation/MITRE ATT&CK/Alert with Mitre ID Details
Mitre by Id	Selects MITRE Ids.	/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre by Id
Mitre by Tactic	Selects MITRE by tactics.	/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre by Tactic

Query Viewers

Name	Description	Location
Alert with Mitre ID Details	Displays details of alerts with MITRE Ids.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/Alert with Mitre ID Details
MITRE by ID	Displays MITRE by Id.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/MITRE by ID
MITRE by Tactic	Displays MITRE by tactic.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/MITRE by Tactic
Mitre Details Summary	Displays MITRE details summary.	/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre Details Summary

Report

Name	Description	Location
Mitre ATT&CK Summary	Displays a summary of MITRE ATT&CK events by MITRE Id, Tactic and Rule.	/All Reports/ArcSight Foundation/MITRE ATT&CK/Mitre ATT&CK Summary

Use Case

Name	Description	Location
Mitre Att&ck Overview	Contains resource for Mitre Att&ck	/All Use Cases/ArcSight Foundation/Mitre Att&ck Overview

Security Threat Monitoring Content

In this appendix, each Security Threat Monitoring resource type has it's own table(s) organized by use case: Application, Cloud, Data, Host, Malware, Network, Perimeter, and Vulnerability Monitoring. These tables have been updated to include 4.0 content.

[Active Channels](#)

[Active Lists](#)

[Dashboards](#)

[Data Monitors](#)

[Fields](#)

[Field Sets](#)

[Filters](#)

[Queries](#)

[Query Viewers](#)

[Rules](#)

[Use Cases](#)

Active Channels

Use Case	Name	Description
Application Monitoring	All DNS Events	Shows all of the DNS Events.
Entity Monitoring	Entity Monitoring Main Channel	Shows all the entity monitoring category correlation events on the last hour.
	Unsuccessful Logins	Shows unsuccessful logins on the last hour.

Active Lists

Some active lists require configuration by the customer, these are marked with an asterisk.

Use Case	Name	Description
Application Monitoring	UAC Suspicious Processes	Tracks UAC Bypass suspicious processes.
Cloud Monitoring	Cloud Accounts Created	Tracks and keeps record of cloud accounts created.
Data Monitoring	Confidential Files*	Fill in the confidential files names list in this active list.
	Exception Email User Domains *	Populate the list of exempted domains in this active list.
Entity Monitoring	Brute Force Attempts	Stores information about suspected "Brute Force IDS Detected Attempts" and "Brute Force OS and Application Attempts." Rules updates this active list with attacker system, user account and target system information.
	User Account Created	Stores the information about the user accounts created within the organization. This active list is used and updated by other Security Threat Monitoring resources. By default, the list expires in 24 hours.

Use Case	Name	Description
	User Accounts Added to Group	Stores the information about the user accounts added to groups within t organization. This active list is used and updated by other Security Threat Monitoring resources. By default, the list expires in 24 hours.
Host Monitoring	Application Monitoring	Tracks the process creations of all processes with explorer.exe as parent.
	Deleted Files On Host	Tracks files deleted from command line on hosts.
	Files Created On Machine	Tracks files created by applications on machine.
Malware Monitoring	Malware Target Based Suppression	Suppression list is based on target address and generator name.
	Suspicious Ransomware Like Activities Tracking	Tracks ransomware-like activities like Shadow Copy Deletion Attempt, Suspicious Access Control List Modifications and Suspicious Boot Configuration Data Modifications.

Dashboards

Use Case	Name	Description
Application Monitoring	DNS DGA Monitoring	Displays DNS DGA Statistics.
	DNS Statistics	Displays Microsoft and AWS Route53 DNS statistics.
Entity Monitoring	Brute Force Attack Detection Dashboard	Displays overview of suspected Brute Force Attacks.
	Members Added and Removed from Privileged Groups	Displays information about members which added and removed from privileged group.
	Unsuccessful Logins from different Countries	Displays overview of unsuccessful logins from different countries.
Malware Monitoring	Malware Activity	Displays malware statistics.
Network Monitoring	Attacks and Suspicious Activity Overview	Displays attacks and suspicious activity based on ArcSight categorization events.
Vulnerability Monitoring	Vulnerability Overview	Displays data related to vulnerable assets.

Data Monitors

Use Case	Name	Description	
Application Monitoring	DNS Domains Not Found	Displays domains that don't exist, high amount of these messages could be a symptom of malware infection on any internal machine.	
	Domains Not Found	Displays domains requested that were not found by the DNS server.	
	Top Addresses Communicating With Malicious Domains	Displays domains requested that were not found by the DNS server.	
	Top DNS Domains Queried	Displays top domains requested.	
	Top DNS Edge Location Resolutions	Displays top AWS edge locations where DNS resolutions have been done.	
	Top DNS Records	Displays top records requested by clients on DNS server.	
	Top DNS Response Codes	Displays top DNS response codes.	
	Top Malicious Domains Accessed	Displays top DGA domains accessed by hosts.	
	Entity Monitoring	All Unsuccessful Logins from different Countries - GeoView	Displays top DGA domains being accessed by hosts.
		Brute Force Attack Attempts	Displays all the unsuccessful logins from different countries on a map.
Members Added and Removed from Privileged Group within 24 Hours		Displays the last 5 brute force attacks attempts.	
Security Indicator - Failed Login Count by User Account		Displays the last 5 members was Added and Removed from Privileged Group within 24 Hours.	
Security Indicator - Most Active Failed Login Source Systems		Displays top 10 counts of failed authentication events, grouped by user account.	
Security Indicator - Systems Experiencing High Volume of Failed Logins		Displays top 10 counts of failed authentication events, grouped by attacker IP address.	
Successful Brute Force Login		Displays the last 5 successful brute force logins.	
Unsuccessful Login Count by Country		Displays top 10 counts of failed authentication events, grouped by source country.	
Malware Monitoring		Latest Malware Infections on Critical Assets	Displays last malware infection on High and Very Critical assets.

Use Case	Name	Description
	Top Addresses With Malware Infections	Displays top addresses having malware infections.
	Top Malware Names Infections	Displays top malware names infecting devices.
Network Monitoring	Attacks and Suspicious Activity per 10 Minutes	Displays a moving average of attacks. It displays data for the last 10 minutes and will generate a correlation event if the moving average is increased by 300%.
	Last 10 Attacks and Suspicious Activity Events	Displays the last 10 attack and suspicious activity events.
	Top 10 Attacker Countries	Displays the top 10 attacker countries.
	Top 10 Attackers	Displays the top 10 attacker IP addresses.
	Top 10 Targets	Displays the top 10 attacks and suspicious activity targets.
Vulnerability Monitoring	Latest Attack on Vulnerable Asset	Displays the latest attacks against vulnerable assets.
	Top Vulnerable Asset under Attack	Displays top assets having vulnerably that are under attack.

Fields

Use Case	Name	Description
Cloud Monitoring	awsAlertAddress	Conditional variable that retrieves source, target or agent address from the event.
	awsAlertAddressZone	Conditional variable that retrieves source, target or agent address zone from the event.
	sourceOrTargetAddress	Conditional variable that retrieves source or target address from event.
	sourceOrTargetAddressZone	Conditional variable that retrieves source or target address zone from the event.
Host Monitoring	getCMDLine	Variable that retrieve the field Destination Service Name if the product is Sysmon else it will return Device Custom String 4 as the command line input.
	getRegistryValue	Variable that retrieves the value set in the registry.
	getTargetProcessName	Variable that retrieves the Target Process name without the path in lowercase.
	FileArchiver	Constant for file archiver category in application list.
	FileTransfer	Constant for file transfer category in application list.

Use Case	Name	Description
	fromSystemDirectory	Variable that checks if the process created is located in the system directory (system32 or syswow64).
	getFileNameFromApplicationsList	Variable that retrieves the active list entries based on the file name.
	getOldFileNameFromApplicationsList	Variable that retrieves the active list entries based on the old file name.
	getOriginalProcessName	Variable that retrieves the field old file name if the product is sysmon.
	getParentPID	Variable that retrieves the parent process ID.
	getParentProcess	Variable that retrieves the field Source Process Name if the product is Sysmon else it will return File Path as the Parent Process.
	getProcessDetails	Variable that retrieves process details.
	getProcessID	Variable that retrieves process IDs.
	getProcessName	Global variable that retrieves the target process name or old file name.
	getTargetProcessNameFromApplicationList	Variable that retrieves the active list entries based on the target process name.
	processName	Variable that retrieves process names.
	suspiciousTrack_JobScheduling	Global variable that concatenates strings for job scheduling tasks.
	suspiciousTrack_ModifyService	Global variable that concatenates strings for suspicious modify services.
	suspiciousTrack_NewService	Variable that retrieves strings of new services.
	suspiciousTrack_ScheduledTask	Variable that retrieves strings of scheduled tasks.
Network Monitoring	getExploitingCategory	Variable that retrieves categories for exploit from a list.
Perimeter Monitoring	getInterZoneCommunications	Variable that retrieves service information from the interzone communications to restricted services list.

Field Sets

Use Case	Name	Description
Application Monitoring	All DNS Events	Contains information related to DNS events.
	DNS DGA	Contains event fields used to investigate DNS DGA events.

Use Case	Name	Description
Entity Monitoring	Brute Force Login	Contains essential fields required to investigate brute force attack through active channels and data monitors.
	Main Channel	Contains essential fields required to investigate Entity Monitoring rules correlation events through active channels.
	Members added and Removed from Groups	Contains essential fields required to investigate members added and removed from groups through active channels and data monitors.
	Unsuccessful Logins	Contains essential fields required to investigate brute force attack through active channels and data monitors.
Malware Monitoring	Malware Events	Contains event fields used to investigate malware events.
Network Monitoring	Attacks and Suspicious Activity	Contains essential fields required to investigate attacks and suspicious activity through active channels and data monitors.
Vulnerability Monitoring	Vulnerable Asset	Contains event field information about asset vulnerabilities.

Filters

Use Case	Name	Description
Application Monitoring	All DNS Events	Detects all the Microsoft and AWS Route53 DNS events.
	AWS Route53 Location DNS Queries	Detects the Route 53 edge location that responded to the query.
	Code Injections from Other Devices	Detects the code injection attacks captured from IDS, Antivirus and other application devices.
	Cross Site Scripting from Other Devices	Detects cross-site-scripting attacks from other device vendors.
	Directory Traversal Attempts from Other Devices	Detects the Directory Traversal attacks captured from IDS, Antivirus and other application devices.
	DNS DGA	Detects events that Microsoft DNS DGA Connector reports as random generate domains used by attackers to evade detection.
	DNS NXDOMAIN Events	Detects NXDOMAIN events from DNS servers.
	DNS Query Codes	Detects DNS query codes.
	DNS Response Codes	Detect DNS response codes.
	DNS SubDomains	Detects DNS subdomains requested.

Use Case	Name	Description
	Format String Attack Attempts from Other Devices	Detects the format strings attacks captured from IDS, Antivirus and other application devices.
	Linux File Inclusions	Detects the most common form of file inclusions to a Linux server during a code injection attack.
	SQL Injection Attempts from Other Devices	Detects the SQL Injection attacks captured from IDS, Antivirus and other application devices.
	Source and Destination Address not Null	Detects events which source and destination address are not null.
	Web Server Activity Events	Detects all Web Server Activity Related Events.
	Windows File Inclusions	Detects the most common form of file inclusions to a Windows server during a code injection attack
Entity Monitoring	A Member was Added and Removed from Privileged Group within 24 Hours	Detects when a user added and removed from a privileged group using windows events on the last 24 hours.
	A Member was Added into a Group	Detects when a user added into a group using windows events.
	A Member was Removed from a Group	Detects when a user removed from a group using windows events.
	Account Creation	Detects account creation events.
	Account Deletion	Detects account deletion events.
	Account Lockouts	Detects account lockouts. By default it will recognize lockouts on Microsoft Windows and Unix systems.
	Security Accounts Manager access tools	Contain the tools which are being used to access the security account manager.
	Login Attempts	Detects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.
	Unsuccessful Logins	Detects failed logins by both administrative and non-administrative users.
	Unsuccessful Logins with Geo Information	Detects failed logins events from different countries with populated Geo fields for both the attacker and target addresses.
	Windows Events with a Non-Machine User	Detects Microsoft Windows events that have a non machine/system user either in the attacker or the target fields.
	Brute Force Attack Attempts	Detects correlation events generated by the rules: <ul style="list-style-type: none"> • Brute Force OS and Application Attempts • Brute Force IDS Detected Attempts

Use Case	Name	Description
	Successful Brute Force Login	Detects correlation events generated by the rule: Successful Brute Force Login.
Host Monitoring	Device Access	Detects events related to devices being accessed.
	Information Transfer to Removable Storage Device	Detects any information transfer to a removable storage device.
	Microsoft Windows Events	Detects Microsoft Windows events.
	Any Process in Application List	Detects events where the process name is in the file names active list.
	File Archiver Process in Application List	Detects events where the process name is in the file names active list with the category file archiver.
	File Transfer Process in Application List	Detects events where the process name is in the file names active list with the category file transfer.
	Removable Device Detected	Detects all removable (storage) devices events by McAfee Data Loss Prevention and Symantec Endpoint Encryption Software.
	Service Failed	Detects service failed events.
	Service Stopped	Detects service stop events.
	Shadow Copy Deletion	Detects shadow copy deletion events.
	Suspicious Access Control List Modifications	Detects suspicious discretionary access control lists modifications
	Suspicious Boot Configuration Data (BCD) Modifications	Detects suspicious boot configuration data modifications.
	File Creation and Modification	Detects file create events.
	Process Create	Detects process create events.
Registry Value Changed	Detects registry value changes.	
Malware Monitoring	Malware Detected	Detects correlation events generated from Malware Detected Rule, such event is an alert about host malware infection.
	Malware Detected - Critical Assets	Detects correlation events generated from Malware Detected Rule on High and Very High critical assets.
Network Monitoring	All IDS Events	Detects all IDS events based on Categorization.
	Attacks and Suspicious Activity	Detects events which indicate compromise, reconnaissance, hostile, or suspicious activity.
	HTRAN Detected	Detects HTRAN signature detected events.

Use Case	Name	Description
Perimeter Monitoring	All Firewall Accept Traffic	Detects events which indicates accepted traffic from firewalls.
	All Firewall Deny Traffic	Detects events which indicates denied traffic from firewalls.
Vulnerability Monitoring	Attack Vulnerable Asset	Detects assets having vulnerabilities.

Queries

Use Case	Name	Description
Entity Monitoring	Last 10 Members Added into a Privileged Group	Pulls the last 10 accounts which added to a privileged groups and not removed within 24 hours.
Malware Monitoring	All Malware Infections	Pulls all malware alerts from Malware Target Based Suppression List.
	Top Addresses With Malware Infections	Pulls top hosts infected from Malware Target Based Suppression active list.
	Top Malware Name Infections	Pulls top malware names infecting devices.
Vulnerability Monitoring	Asset Vulnerability	Pulls assets associated with vulnerabilities.

Query Viewers

Use Case	Name	Description
Entity Monitoring	Members Added into a Privileged Groups	Displays the last 10 accounts which added to a privileged groups and not removed within 24 hours.
Malware Monitoring	All Malware Infections	Displays all malware alerts.
	Top Addresses With Malware Infections	Displays top addresses with malware infections.
	Top Malware Name Infections	Displays top malware names infecting devices.
Vulnerability Monitoring	Asset Vulnerability	Displays assets with vulnerabilities.

Rules

Security Threat Monitoring provides you with many rules to help protect your environment, so each use case has its own table.

 **Note:** To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

Application Monitoring

Name	Description
Abnormal Use of hh.exe	Detects abnormal use of hh.exe command.
An Attempted Access to Lsass.exe	Detects adversaries trying to access "Lsass.exe."
API Hooking Detected	Detects API hooking using volatility apihooks plugin.
CMSTP Involved on Network Connection	Detects network connections initiated by CMSTP.exe.
Code Execution Through .lnk File	Detects malicious code executed by .lnk file.
Credential Dumping through Keefarce	Detects credential dumping practiced through Keefarcec.
Detected Code Injection	Detects code injection attacks to the application server via the request URLs, also from other IDS and application devices.
Detected Cross Site Scripting	Detects cross site scripting attacks to the application server via the request URLs and also from other IDS and application devices.
Detected Directory Traversal	Detects directory traversal attacks.
Detected DLL Hijacking Activity by PowerSploit	Detects DLL Hijacking activity by powersploit.
Detected DLL Injection by Mavinject.exe	Detects DLL injection by Mavinject.exe.
Detected Enabled DCOM	Detects if DCOM is enabled on the system using vulnerability scanner events.
Detected Format String Attack	Detects format strings attacks.
Detected SQL Injection	Detects SQL Injection attacks to the application server via the request URLs and also from other IDS and application devices.
Detected Squiblydoo Attack	Detects Squiblydoo attacks.

Name	Description
Dynamic Data Exchange Related Attack	Detects attacks leveraging Dynamic Data Exchange (DDE) technology.
Execution of Processes with Trailing Spaces	Detects execution of linux processes with trailing spaces.
Execution through Module Load	Detects exploit execution through DLL.
Exploit of Client Application	Detects execution of exploit on client applications (like web browsers, Microsoft Office, Adobe Reader and Flash).
File Transfer Using TeamViewer	Detects remote file transfers due to the use of TeamViewer application.
HTA File Download	Detects hosts trying to download an .HTA file.
Image File Execution Options Injection	Detects image file execution options injection through reg.exe command.
InstallUtil Involved on Network Connection	Detects network connections initiated by InstallUtil.
JavaScript Code Executed through rundll32	Detects JavaScript code executed through rundll32.
Malicious Control Panel File Detected	Detects malicious control panel files
Malicious PowerShell Commandlets	Detects malicious PowerShell commandlets running on your environment.
Masquerading Through Unicode Right-To-Left Override (RTLO)	Detects masquerading attempts through unicode right-to-left override (RTLO).
MSBuild.exe Executed on Non Development Environment	Detects MSBuild.exe execution on non-development machine.
Mshta Command Execution	Detects Mshta command executions.
MSXSL.exe Detected on Non Development Environment	Detects MSXSL.exe on non-development environment.
Multiple Access Attempts To Malicious Domains From Same Source Address	Detects multiple access attempts on malicious domains from same source address.
Multiple RDP Connections from the Same Host in Short Period of Time	Detects multiple RDP connections from the same host in short period of time.

Name	Description
Multiple RDP Connections from the Same User in Short Period of Time	Detects detects multiple RDP connections from the same user in short period of time.
New Child Process Launched by CMSTP	Detects when a new child process is launched by CMSTP.exe.
New Child Process Launched by WMIIPRVSE.EXE	Detects when a process spawns from wmiiprvse.exe.
New Process Created by InstallUtil	Detects when a new process is created by Installutil.
NXDOMAIN Attack	Detects multiple DNS queries to non-existing domains from same source address.
Obfuscated PowerShell Detected	Detects obfuscated PowerShell execution.
Possible Application Shimming PE Original Filename and Hash Indicator	Detects sdbinst.exe original PE File name or Hash Detected.
Possible Credential Dumping	Detects when a process tries to access lsass.exe
Possible Macro Embedded on Office Document	Detects when a macro embeds in an Office document.
Possible Masquerading Detected	Detects possible masquerading of processes.
Possible Process Hollowing by PowerShell	Detects process hollowing by PowerShell.
Possible Process Injection by PowerShell	Detects process injection by powershell.
Possible Screen Capture by PowerShell	Detects screen captures by PowerShell.
Powershell Invoke-command Executed on Remote Host	Detects PowerShell invoke-commands executed on a remote host.
Powershell Script Executed by SyncAppvPublishingServer	Detects powershell scripts executed by SyncAppvPublishingServer.
RDP Over a Reverse SSH Tunnel	Detects RDP connections over a reverse SSH tunnel using plink.exe or equivalent utilities provides the attacker a convenient pseudo VPN access method, via which adversaries may use more systems with less noise and least footprint.

Name	Description
Regsvcs OR Regasm Making Network Connection	Detects network connections initiated by Regsvcs/Regasm.
Remote Access Tool Detected	Detects remote access tools.
Remote Access Tool Downloaded Using PowerShell	Detects remote access tools are downloaded using PowerShell.
Remote PowerShell Session Activity On Host	Detects remote powershell sessions established on a host.
sdclt Suspicious Process Detected	Detects sdclt suspicious processes.
Shell Command Execution	Detects the execution of potential shell commands and shellcode attacks.
Sudo Command Execution Detected	<p>Detects sudo command executions.</p> <p>Linux Note:To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <p>-a exit,always -F arch=b64 -F euid=0 -S execve</p> <p>-a exit,always -F arch=b32 -F euid=0 -S execve</p> <p>Restart the audit service.</p>
Suspicious Large DNS Domain Requested	Detects long DNS queries. Long queries are sometimes used for data exfiltration or C2 communication.
Suspicious Powershell Command Line Argument Detected	Detects suspicious powershell command line arguments.
Suspicious RDP Redirection Using TSCON	Detects RDP session redirection using TSCON. Adversaries can hijack a session without the need for credentials or prompts to the user. This could be done remotely or locally and with active or disconnected sessions.
Suspicious Use of Msiexec.exe	Detects suspicious use of Msiexec.exe.
Suspicious Use of MSXSL.EXE	Detects suspicious use of msxsl.exe.
Suspicious Use of PubPrn.vbs	Detects suspicious use of PubPrn.vbs.
Suspicious Use of WMIC	Detects suspicious use of wmic.exe.
TeamViewer Logging Disabled	Detects when TeamViewer logging is disabled. Adversaries may disable TeamViewer Logging to avoid possible detection of their activities.

Name	Description
UAC ByPass through sdclt.exe	Detects UAC Bypass through sdclt.exe. Make sure rule "sdclt.exe Suspicious Command Executed" is enabled before using this rule.
VNC Exploit Execution	Detects the execution of potential exploits on vnc related software.
Windows Remote Management Enabled by PowerShell	Detects if Windows Remote Management is enabled using powershell.

Cloud Monitoring

Name	Description
AWS Account Privilege Escalation Activity	Detects anomalous API requests associated with privilege escalation activity observed from any AWS cloud account.
AWS Brute Force Activity from EC2 Instance	Detects AWS suspicious brute force activity on EC2 instance.
AWS DoS Activity from EC2 Instance	Detects AWS DoS activity from EC2 instance.
AWS EC2 Bitcoin Activity	Detects AWS EC2 instances found querying IP addresses or domains associated with Cryptocurrency activity.
AWS EC2 Unusual Port Traffic	Detects when an EC2 instances established a communication on an unusual port.
AWS Exfiltration Activity	Detects suspicious activity related to exfiltration on the AWS cloud environment.
AWS Impossible Travel	Detects multiple successful console logins for the same IAM user occurred around the same time in various geographical locations.
AWS Instance Querying DGA Domains	Detects when an AWS EC2 instance is querying DGA domains.
AWS Password Policy Changed	Detects when a password policy weakens on AWS cloud account.
AWS Pentest Activity	Detects penetration testing tools used on AWS cloud accounts to make unauthorized API requests on the cloud.
AWS Phishing Activity from EC2 Instance	Detects suspicious activity related to phishing or Spam on EC2 instances.
AWS Port Scan	Detects AWS port scan activity on EC2 instance.

Name	Description
AWS Root Account Usage	Detects AWS suspicious activity on root accounts.
AWS S3 Policy Misconfiguration	Detects suspicious activity related to AWS S3 policy misconfiguration.
AWS S3 Unauthorized Access	Detects suspicious activity related to AWS S3 unauthorized access.
AWS Unusual Policy Changes on S3 buckets	Detects abnormal permission policy changes on S3 Buckets.
Azure Resource Group Deleted	<p>Detects when azure resource groups are deleted.</p> <p>Investigation Tip: Adversaries could delete resource groups to disrupt the environment or to destroy data, therefore investigate if deletion was done by an authorized account.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Azure Runbook Created	<p>Detects when an azure runbook is created in the cloud environment.</p> <p>Investigation Tip: Adversaries could create runbooks to execute automate tasks in the azure cloud environment.</p> <p>False Positives: Cloud administrator executing administrative tasks in the cloud environment.</p>
Azure Runbook Deleted	<p>Detects when an azure runbook is deleted in the cloud environment.</p> <p>Investigation Tip: Adversaries could delete existing azure runbooks to disrupt certain functionalities within the cloud environment.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Azure Service Principal Created	<p>Detects when an azure service principal is created.</p> <p>Investigation Tip: Adversaries could abuse of service principals and use it as backdoors to consistently access the environment and carry out malicious activities. Monitor service principals and ensure this is created by an authorized account.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Cloud Account Created	<p>Monitors all the user accounts created on the cloud environment. This rule tracks users accounts created in the Active list Cloud Accounts Created then the information will be used by other use cases as support for chaining conditions so that the amount of possible false positives can be reduced. Every user account tracked in the active list will be only by 24 hours as default and after this time the record will be automatically removed.</p>
Cloud Firewall Deleted	<p>Detects when any of the firewall features provided by the cloud vendor it is disabled or deleted.</p> <p>False Positive: Regular activity performed by cloud administrators.</p>

Name	Description
Cloud Instance Created By Recent User Created	<p>Detects when cloud instances are created by a user account recently created in the cloud environment. The user that created an instance must be on the active list Cloud Accounts Created to produce an alert.</p> <p>False Positives: A new administrator account created creating cloud instances.</p>
Cloud Instance Deleted By Recent User Created	<p>Detects when cloud instances are deleted by a user account recently created in the cloud environment. The user that deleted the instance must be on the active list Cloud Accounts Created to produce an alert.</p> <p>False Positives: A new administrator account deleting cloud instances.</p>
Cloud Instance Snapshot By Recent User Created	<p>Detects when cloud snapshots are created by a user account recently created in the cloud environment. The user that created the snapshot must be in the active list Cloud Accounts Created to produce an alert.</p> <p>False Positives: A new administrator account creating cloud snapshots.</p>
Cloud Key Vault Deleted	<p>Detects when cloud key storage has been deleted on the cloud environment.</p> <p>Investigation Tip: Find out if the user deleting the key vault is authorized to do such activity.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Cloud Key Vault Updated	<p>Detects when cloud key storage modified or created on the cloud environment.</p> <p>Investigation Tip: Find out if the user updating or creating the key vaults is authorized to do such activity.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Cloud Monitoring Disabled	<p>Detects when cloud monitoring has been disabled or deleted from the environment.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Cloud Network Monitoring Disabled	<p>Detects when network diagnostic settings have been disabled or deleted on the cloud environment.</p> <p>Investigation Tip: Find out if the user account is authorized to carry out any of these activities.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Cloud Storage Deleted	<p>Detects when cloud storage was deleted.</p> <p>Investigation Tip: Adversaries could delete resource groups to disrupt the environment or to destroy data. Investigate if the deletion was done by an authorized account.</p> <p>False Positives: Administrator account doing maintenance in the cloud environment.</p>
Email with Malicious Url	<p>Detects emails with malicious Url on Office 365.</p>

Name	Description
Multiple Cloud Firewall Updates	<p>Detects when multiple cloud firewall updates are made by same user account in a short period of time.</p> <p>False Positives: Regular Administrator cloud account user performing changes on the environment.</p>
SharePoint Activity by Privileged User	Detects files are accessed by a privileged username. You can customize the privileged user account with upper case on the list /All Active Lists/ArcSight Foundation/Common/Privilege User Account.
Suspicious SharePoint Activity	Detects large amount of files accessed by the same username in a short period of time.

Data Monitoring

Name	Description
Data Loss through Clipboard Data	Detects data loss from clipboard data.
Data Loss through Email	Detects data loss from the outgoing emails.
Data Loss through Email Redirect	Detects data loss through email redirects.
Data Loss through Network Shared Drive	Detects data loss occurred through network shared drive.
Data Loss through Screen Capture	Detects data loss occurred through screen capture.

Entity Monitoring

Name	Description
A Member was Added and Removed from Privileged Group within 24 Hours	Detects users added and removed from a privileged group within 24 hours using windows events.
A Member was Added into a Privileged Group	Detects users added into a privileged group using windows events.
A user account was terminated	Tracks the accounts which are being deleted from the active directory.
Account Tampering - Suspicious Failed Logon	Detects uncommon error codes on failed logins that occurred due to suspicious activity or tampering with accounts.
Authentication Attempted to Disabled Account	Detects authentication attempts on a disabled account.

Name	Description
Brute Force IDS Detected Attempts	Detects brute force attack attempts detected by IDS. The rule triggers when ArcSight manager receives a brute force attack attempt event from IDS. On first event, the user account, attacker system and target system information is added to "Brute Force Attempts" active list.
Brute Force OS and Application Attempts	Detects brute force attacks on OS and applications. The rule triggers when the failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold. On first threshold, information about user account, attacker system and target system is added to "Brute Force Attempts" active list.
Consecutive Unsuccessful Logins to Administrative Account	Detects sets of 5 consecutive unsuccessful logins to privilege account within 1 minute.
Consecutive Unsuccessful Logins to Same Account from different Countries	Detects sets of 3 consecutive unsuccessful logins to the same account from 3 different countries.
Consecutive Unsuccessful Logins to Same Account from different IPs	Detects sets of 3 consecutive unsuccessful logins to the same account from 3 different IP addresses.
Default Account Enabled	Detects when a default account has been enabled.
Log into Multiple Systems in Short Period	Detects logins into multiple systems in short time period.
Login after Work Hour	Detects logins after work hour.
Multiple Attempts to Discover User Accounts	Detects attackers trying to discover multiple user accounts present in local and security groups.
Multiple Failed Login to Different Accounts from Single Source	Detects multiple failed logins to different accounts from the same source.
Privileged Account Locked Out	Detects account lockouts.

Name	Description
Security Accounts Manager accessed through unauthorized tools	Creates a correlation event when the security accounts manager is accessed through unauthorized tools.
Successful Brute Force Login	Detects successful authentication events after suspected brute force attempt. The rule triggers when the user account, attacker system and target system information of successful authentication event matches an entry in the "Brute Force Attempts" active list.
Terminated User Account Added to the Privileged Group	Detects terminated user accounts added to the privilege group.
Terminated User Account Successful Logon Detected	Creates a correlation event when the successful login by terminated user account is detected.
User Account Created	Detects when a user account is created.
User Account Created and Deleted within 24 Hours	Detects the anomalous behavior of user account creation and then deletion within 24 hours (Default TTL: 24 Hours). The rule triggers a correlation event send to a Triage main channel. This rule uses an active list.

Host Monitoring

Name	Description
Access Token Manipulation by Powersploit	Detects Access Token Manipulation practiced through Powersploit.
Active Directory Database Dumping via Ntdsutil	Detects NTDSUtil tool dumping a Microsoft Active Directory database to disk.
AD Object Permission Enumerated	Detects adversaries trying to enumerate the permissions of AD object
AD Reconnaissance through AdFind	Detects when the Adfind tool is used for reconnaissance in an Active Directory environment. Adfind is used to query the local password policy.
Audit Cleared Log	Detects an audit-log-cleared event, upon each detection the rules adds target address in suppression list in order to avoid multiple alerts on same address in a short period of time.
Browser's Saved Credentials Access Detected	Detects adversaries trying to access the saved credentials from the browser, currently limited to Chrome, Mozilla, Opera, and IE.

Name	Description
Browser's Saved Credentials Dumping Attempt by PowerShell	Detects PowerShell modules or cmdlets trying to dump browser's saved credentials based on PowerShell events.
Brute Force Password Protected Office Files	Detects multiple failed attempts to a password protected microsoft office files like doc, excel and pptx.
CertUtil used to decode file on host	Detects certutil usage to decode files.
Chained Rule - System Information Discovery	<p>Detects attempts to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.</p> <p>Linux Note: In order to capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p>Restart audit service.</p> <p>Windows Note: To capture the Windows logs,enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Changes to Windows Firewall Exception List	<p>Detects modifications to the windows system firewall exception list.</p> <p>Windows Note: In order to capture the windows logs, follow the steps below.</p> <p>Enable auditing in the following fields in the group policy editor:</p> <p>Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change.</p> <p>Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields:</p> <ul style="list-style-type: none"> • Audit Filtering Platform Policy Change • Audit MPSSVC Rule-Level Policy Change • Audit other Policy Change EventsRestart the service mpssvc.

Name	Description
Commands Executed to Create a New Service	<p>Detects abuse to the system via the creation of new services using Command Line tool or PowerShell.</p> <p>Windows Note: To capture the Windows logs,enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
COR_PROFILER to Hijack Program Execution Flow	<p>Detects leveraging of the COR_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded.</p> <p>WindowsNote: To capture the Windows logs,enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Crackmapexec Pass the Hash	<p>Detects Pass the hash (PtH) occurs using crackmapexec.</p>
Credential Dumping via ProcDump and Task Manager	<p>Detects when the ProcDump is used to dump the memory space of Lsass.exe and when credential dumping through window task manager is practiced.</p>
Credentials in Group Policy Preferences	<p>Detects attempts to find unsecured credentials in Group Policy Preferences (GPP).These group policies are stored in SYSVOL on a domain controller. This means that any domain user can view the SYSVOL share and decrypt the password (using the AES key that has been made public). Learn more at:https://attack.mitre.org/techniques/T1552/006/</p> <p>Windows Note: To capture the Windows logs,enable command-line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>

Name	Description
Credentials in Registry Discovery	Detects queries to the Registry looking for credentials and passwords that have been stored for use by other programs or services. WindowsNote: To capture the Windows logs,enable command-line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
Data Collection through Mimikittenz	Detects Data Collection attempts via Mimikittenz. Mimikittenz is a post-exploitation PowerShell tool that utilizes the Windows function ReadProcessMemory() to extract plain-text passwords from various target processes.mimikittenz can also easily extract other kinds of juicy info from target.
Data Compression Process Started on Critical Host	Creates a correlation event when a process from the applications active list is started on a critical host.
Data Encoding Using Certutil	Detects when a file has been encoded using Certutil.
Data Likely Staged for Exfiltration	Detects data staged into a centralized location.
DCOM Instance Creation Attempted	Detects DCOM instance creation attempts via PowerShell.
DCOM Objects Enumeration via PowerShell	Detects enumeration ofDCOM objects via PowerShell.
Disable System Firewall Using PowerShell	Detects disabling of the windows system firewall. Enable auditing of Windows PowerShell events in order to capture the logs.
Disable System Firewall Using Registry Keys	Detects disabling of the windows system firewall. Enable auditing of Windows PowerShell events in order to capture the logs.

Name	Description
Disable Windows System Firewall	<p>Detects disabling of the windows system firewall.</p> <p>Windows Note: In order to capture the windows logs, follow the below steps.</p> <p>In order to audit any policy changes in windows, enable auditing in the following fields in the group policy editor:</p> <p>Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change.</p> <p>Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields:</p> <ul style="list-style-type: none"> • Audit Filtering Platform Policy Change • Audit MPSSVC Rule-Level Policy Change • Audit other Policy Change Events Restart the service mpssvc.
Disabled tty_tickets for Sudo Caching	<p>Detects disabling of tty_tickets for sudo caching.</p> <p>Snoopy Note: In order to capture this use case please enable Snoopy Logging in the machine (or) simply provide the path /var/log/secure by installing the syslog file connector on the machine to be monitored.</p>
DNS-Tunnel Creation Attempted via DNScat	<p>Detects when DNScat is downloaded and DNS Tunnel Creation is Attempted.</p>
External Device With autorun.inf Detected	<p>Detects external drives plugged having autorun.inf</p>
File Copied On Shared Folder	<p>Detects files copied on a shared folder. In order to get these events, you must enable folder auditing in Windows.</p>
File Downloaded On Host	<p>Detects files downloaded using a web browser on the host.</p>
File or Folder deleted by PowerShell	<p>Detects possible file or folder deletion by PowerShell.</p>
File or Folder Deleted Using cmd.exe	<p>Detects Windows deletion of files and folders using cmd.exe / c.</p>
File or Folder Deletion on Linux	<p>Detects attempts to delete files and folders on the Linux system.</p> <p>To capture this use case, the following steps are needed to be done:</p> <ol style="list-style-type: none"> 1. Install Snoopy Logging (open source) on the Linux machine that is being monitored. 2. Install Syslog file connecto. 3. Provide the path as /var/log/secure in the Syslog connector

Name	Description
Fileless UAC Bypass Using sdclt.exe	Detects user access bypass practiced through sdclt.exe.
Files Created	Tracks files created by browser and mail applications.
Files Deleted On A Host	Tracks files deleted from a command line interface on a host.
Host Firewall Has Stopped	Detects when host firewall service has stopped on host.
Indirect Command Execution	Detects when forfiles.exe or pcalua.exe is being used to run a process.
Information Collection through Keystroke Applications	Detects Input Capture technique practiced through Keystroke Applications.
Information Transfer to Removable Device	Creates a correlation event when information is transferred to a removable external device.
Information Transfer to Removable Storage Device	Creates a correlation event when information is transferred to a removable external device.
Inhibit System Recovery	Detects when built-in operating system services designed to help in recovery are disabled or deleted.
Invoke-DCOM Attempted via PowerShell	Detects invoke-DCOM commands run via PowerShell on remote hosts via COM objects over DCOM.
Juicy-Rotten-Rogue Potato Exploitation	Detects privilege escalation using Juicy, Rotten and Rogue potato exploitation.
Key Created At Image File Execution Options Registry Folder	Detects keys created at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option.
Key Created At Silent Process Exit Registry Folder	Detects keys created at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\.

Name	Description
Keystrokes Logging Attempt by PowerShell	Detects PowerShell modules and cmdlets trying to log keystrokes.
Large amount of file modifications in users directories	Detects large amounts of file creation/modification in user directories.
Large Information Transfer to Removable Storage Device	Creates a correlation event when a large file transfer to a removable storage device has been detected.
Linux Auditd Kernel Module Loaded in Critical Server	Detects the loading of Linux kernel modules. This rule needs special instructions to install the connector and configuration log: https://sec.microfocus.com/foswiki/bin/view/ArcSightActivate/PLinuxOSConnectorInstallation .
LoggedOn Users Enumeration Detected	Detects when logged-on user enumerations are performed via cmd and PowerShell.
Logging Service On Host Has Stopped	Detects when logging has stopped on host.
Malicious process Masquerading as Windows Process	Detects malicious files running as a windows-known list of process from a different place other than c:\windows\system32.
Mark-of-the-Web Bypass Using PowerShell	Detects abuse of specific file formats to subvert Mark-of-the-Web (MOTW) controls.
MetaSploit Detected	Detects Metasploit framework installation on the system using assessment tools.
Multiple Access To Windows Default Shared Folders From Same Source Address	Detects when the same source address tries to access default windows admin share folders on multiple devices.
Multiple Services Down on Same Host	Detects multiple services down on same host in a 30 minutes lapse. Upon each detection, the rule adds the target address to the suppression list in order to avoid multiple alerts on same address in a short period of time. This rule is disabled by default due to possible performance impact.

Name	Description
Named Pipe Filename Local Privilege Escalation	Detects the practice of the named pipe impersonation.
New Command-Line Session	Detects new command-line sessions are launched.
New Powershell Session	Detects new powershell sessions are launched.
New Scheduled Task Created	Detects new scheduled tasks created using windows events. Windows Event 602 also covers changes to the scheduled task.
New Scheduled Task Via Schtasks	Detects new scheduled tasks created through schtasks.exe command.
New Self-Signed Certificate Created using PowerShell	Detects attempts to create a new Self-Signed Certificate using PowerShell by an insider.
New Service Installation Detected	Detects new service installations reported by windows security event 4697.
New Service Installation Reported by SCM	Detects new service installations reported by security control manager.
Odbcconf to Proxy Execution of Malicious Payloads	<p>Detects abuse odbccconf.exe to proxy execution of malicious payloads. Odbccconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names.</p> <p>Windows Note: To capture the Windows logs, please enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Pass The Hash	Detects Pass The Hash attack attempts on Windows machines. Upon each detection, the rules adds the target address to the suppression list in order to avoid multiple alerts on same address in a short period of time.

Name	Description
Possible Application Shimming New Shim DataBase Indicator	Detects new shim database files created in the default shim database directory.
Possible Application Shimming Process Execution Indicator	Detects the execution of sdbinst.exe.
Possible Application Shimming Registry Indicator	Detects changes to entries relevant to application shimming.
Possible Application Window Discovery	Detects application window discovery activity on hosts.
Possible Archive of Collected Data Using PowerShell	<p>Detects data compression collected using PowerShell.</p> <p>Windows Note: To capture the Windows logs, please enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Possible Change of Default File Association	<p>Detects malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked.</p> <p>Windows Note: To capture the Windows logs, please enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Possible DCSync OS Credential Dumping	Detects DCSync OS credential dumping based on windows event 4662, for more information about this event refer to https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4662 .

Name	Description
Possible Domain Account Created	Detects domain accounts created from the command line interface on a computer.
Possible Domain Account Discovery	Detects domain account discovery activity.
Possible File and Folder Discovery On Linux	Detects multiple commands related to file and folder discovery are run on same Linux machine in a short time.
Possible File And Folder Discovery On Windows Machine	Detects possible activity related to file and folder discovery on the host.
Possible Network Share Discovery	Detects network share discovery activity.
Possible Remote File Copy From Command Line	Detects files copied over the network from CLI.
Possible Software Packing Attempted	Detects Software Packing attempts through UPX and Mpress packers.
Possible System Owner Discovery	Detects system owner discovery activity on the machine.
Possible WMI Persistence	Detects possible WMI persistence activity on the machine.
Potential Privilege Escalation via Unquoted Service	Detects when an Unquoted Service vulnerability is compromised.
PowerShell Antivirus Software Discovery	Detects Powershell usage to list the anti-virus software on machine.
PowerShell Executed From Browser	Detects powershell execution from a browser.
Powershell Related Alert	Detects powershell related alerts.

Name	Description
Privilege Escalation through PrintSpoofer	Detects impersonation privilege abuse on Windows 10 and server 2019.
Process Discovery Using PowerShell	Detects when adversaries look for information about running processes on a system using PowerShell Command.
Process Spawned by PsExec	Detects processes spawned by PsExec.exe.
Proxy Modification Attempt	Detects attempts to change the proxy settings using netsh.
Proxy Server Address Modified	Detects when HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer values is modified.
PsExec Tool Execution	Detects execution of sysinternals PsExec tools.
Registry Modified by Reg.exe	Detects registries modified by reg.exe command line.
Registry Modified Using PowerShell	<p>Detects adversaries looking for information about running processes on a system.</p> <p>Linux Note: In order to capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p>Restart audit service.</p>
Remote File Copy Using Certutil.exe	Detects certutil.exe used to download file from the internet.
Removable Device Blocked On Host	Detects when a removable device is blocked on a host.
Scheduled Task Deleted	Detects the deletion of scheduled tasks.
Script Executed On Critical Host	Detects scripts executed on a critical host.

Name	Description
Service Modified through Registry Using PowerShell	Detects adversaries modifying system services through registry using powershell commands.
Shadow Copy Deletion Attempt	Adds events with process command line parameters containing commands to delete the shadow copies to the suspicious ransomware activities tracker active list.
Signed Binary Proxy Execution	<p>Detects adversaries might bypass process and signature-based defenses by proxying execution of malicious content with signed binaries.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing"</p>
Sudoers File Modified	<p>Detects adversaries trying to modify the sudoers file in the Linux system.</p> <p>Linux Note: To capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <p>-a exit,always -F arch=b64 -F euid=0 -S execve</p> <p>-a exit,always -F arch=b32 -F euid=0 -S execve</p> <p># For monitoring particular file location, we have to add the below rule to the file -w /etc/sudoers -p w -k sudoers_file_modified Here, -w stands for the file path monitoring hosts location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. retain the name as "sudoers_file_modified", because we have used the same string name in one of the variable in the rule condition to catch these events.</p> <p>Restart the audit service.</p>
Suspicious Access Control List Modifications	Adds suspicious discretionary access control lists modifications events to the suspicious ransomware activities tracking active list.
Suspicious Activity after Local Job Changes	Detects suspicious activities after local scheduled job is changed.
Suspicious Activity after Modify Service	Detects suspicious activities after modifying a service.

Name	Description
Suspicious Activity after New Service	Detects suspicious activities after adding new service.
Suspicious Activity after Scheduled Task	Detects suspicious activities after scheduled task is created or updated.
Suspicious Application Discovery Activity On A Host	Detects multiple queries done to the registries that contain information about applications installed on a host.
Suspicious Boot Configuration Data Modifications	Adds suspicious Boot Configuration Data modifications events to the suspicious ransomware activities tracker active list.
Suspicious Commonly Used Port Events by Script	Detects commonly used port event launched by a script.
Suspicious Data Compression Process Started From Command Line	Creates a correlation event when a process from the applications active list is started from the command line.
Suspicious Data Encryption Process Started From Command Line	Creates a correlation event when a process from the applications active list is started from the command line using encryption parameters.
Suspicious Data Transfer Process Started From Command Line	Creates a correlation event when a process from the applications active list is started from the command line.
Suspicious Executable File with Double Extension	Detects when a windows executable file has a double extension.
Suspicious File Created	Detects suspicious files created on the host.
Suspicious File Discovery Activity On Host	Detects multiple file extensions accessed on the same machine in short period of time.

Name	Description
Suspicious net use usage detected	Detects windows admins used in the command net use.
Suspicious Network Connections From Rundll32 Process	Detects rundll32.exe processes initiate a network connection to an IP address outside protected company range.
Suspicious Process Launched By User	Detects user executions of suspicious files.
Suspicious Process Launched From Microsoft Office Applications	Detects uncommon processes launched from Microsoft office applications.
Suspicious Process Run Location	<p>Detects windows processes executed from suspicious locations.</p> <p>In Windows, files should never execute out of certain directory locations. Any of these locations may exist for a variety of reasons, and executables may be present in the directory, but should not execute.</p>
Suspicious Remote Desktop Protocol	Detects suspicious RDP commands.
Suspicious Remote System Discovery Commands Entered On Linux	Detects when remote system discovery commands are entered on Linux machine.
Suspicious Remote System Discovery Commands Entered On Windows	Detects when remote system discovery commands are entered on Windows machine.
Suspicious Uncommonly Used Port Events by Script	Detects commonly used port event launched by a script.

Name	Description
System Information Discovery	<p>Detects adversaries attempting to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.</p> <p>Linux Note: To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve</pre> <pre>-a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p>Restart audit service.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing"</p>
System Process Discovery	<p>Detects adversaries looking for information about running processes on a system.</p> <p>Linux Note: In order to capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve</pre> <pre>-a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p>Restart audit service.</p>
Track Job Scheduling Change	<p>Detects changes of the file /etc/crontab.</p>
Track Modified Service	<p>Tracks modified services.</p>
Track New Service	<p>Tracks new services.</p>
Track Scheduled Task	<p>Tracks schedule tasks and writes them down on Suspicious Activities Tacking Active List.</p>
UAC ByPass Registry Key Changed	<p>Detects changes to an entry relevant to UAC Bypass.</p>

Name	Description
Unlimited Sudo Cache Timeout Set	<p>Detects when an adversary sets unlimited sudo cache timeout.</p> <p>Note: In order to capture this use case enable Snoopy Logging in the machine (or) simply provide the path /var/log/secure by installing the syslog file connector on the machine to be monitored.</p>
Unusual Microsoft Office Network Connections	<p>Detects unusual traffic generated by Microsoft Office applications.</p>
Unusual Windows Process Relationship	<p>Detects unusual parent - child windows system process relationships.</p>
Virtual Machine Environment Discovery Using Registry	<p>Detects when an adversary interacts with the Windows Registry to gather information about the system, configuration, and installed software.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Windows Admin Share Accessed	<p>Detects when a windows admin shared has been accessed.</p>
Windows File Deleted Using Sdelete	<p>Detects Sdelete command executions.</p>
Windows Firewall Rule Changed by netsh command	<p>Detects windows firewall rule changed by netsh command.</p>
Windows Firewall Rule Discovery	<p>Detects queries made on registry that keeps Windows Firewall Rules.</p>

Name	Description
Windows Hooking API Used by PowerShell	Detects windows hooking API used by powershell.
Windows Registry Run Keys and Startup Folder	Detects entries added to the run keys in the registry or startup folder.
WMI Command Executed	<p>Detects adversaries trying to abuse Windows Management Instrumentation (WMI) to achieve execution.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>

Malware Monitoring

Name	Description
Dynamic Data Exchange Malware Detected	Detects dynamic data exchange malware activities on the devices.
External Device On Machine Infected With Malware	Detects malware infections on a machine where an external drive was plugged with autorun.inf.
File Deleted On Malware Infected host	Detects files are deleted on a malware infected host.
Malware Detected	Detects malware activities on the devices, upon each detection the rule adds target address in suppression list in order to avoid multiple alerts on same address in a short period of time.
Malware Detected On File Downloaded on Machine	Detects malware activity on files downloaded on the device by an user, therefore if there is a malware infection and file exists on the active list and further analysis on the machine will be required.

Name	Description
Malware Detected on localhost	Detects malware activities on the devices, upon each detection the rule adds the hostname in suppression list in order to avoid multiple alerts from the same host in a short period of time.
Possible Ransomware Detected	Triggers when one of the following conditions are met: <ul style="list-style-type: none"> • Large file modifications in the users directory and (shadow copy deletion attempt or suspicious access list modifications or suspicious boot configuration data modifications) • Two different events from (shadow copy deletion attempt, suspicious access list modifications, suspicious boot configuration data modifications).
Registry Injection	Detects modifications on Appinit_DLL, AppCertDlls and IFE0 (Image File Execution Options) which are registry keys that malware usually modify for injection and persistence.

Network Monitoring

Name	Description
Browser Bookmark Discovery	Detects adversaries trying to enumerate browser bookmarks to learn more about compromised hosts. Browser bookmarks might also highlight additional targets after an adversary has access to valid credentials, especially credentials in files associated with logins cached by a browser. Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing "
Domain Trust Discovery	Detects adversaries attempting to gather information on domain trust relationships that may be used to identify opportunities in Windows multi-domain/forest environments. Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths. Administrative Templates\System\Audit Process Creation Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing "
DoS Activity Detected by IDS	Detects Network Denial of Service attacks gathering information from IDS.
Exploit Attempt Detected by IDS	Detects exploit attacks through various ways gathering information from IDS.

Name	Description
High Severity IDS Event	Detects high severity exploit attacks simulated through various ways gathering information from IDS.
HTRAN Signature Detected	Detects HTRAN signatures that proxy connections through intermediate hops and aids adversaries in hiding their true geographical locations.
Modification of Password Domain Policy	<p>Detects adversaries attempting to access and modify detailed information about the password policy used within an enterprise network. This helps the adversary to create a list of common passwords and launch dictionary and brute force attacks .</p> <p>Linux Note: To capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p># For monitoring particular file location, we have to add the below rule to the file:</p> <pre>-w /etc/login.defs -p wa -k password_policy_modified -w /etc/pam.d/system-auth -p wa -k password_policy_modified</pre> <p>Here, -w stands for the file path monitoring password policy files location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. retain the name as "password_policy_modified", because we have used the same string name in one of the variable in the rule condition to catch these events.</p> <p>Restart audit service.</p>
Multiple Queries to Registry for Discovery	<p>Detects adversaries interacting with the Windows Registry to gather information about the system, configuration, and installed software.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p>
Multiple Unique IDS Events to Same Destination	Detects multiple unique IDS events gathering information from IDS. This rule triggers only where there are 4 unique IDS events in a span of 30 minutes to the same destination.
Outbound SSH Connection Detected	Detects outbound SSH connections.

Name	Description
Password Policy Discovery	<p>Detects adversaries attempting to access detailed information about the password policy used withing an enterprise network. This action helps adversaries create a list of common passwords and launch dictionary and brute force attacks.</p> <p>Linux Note: To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p># For monitoring particular file location, we have to add the rule below to the file:</p> <pre>-w /etc/login.defs -p rx -k password_policy_discovered -w /etc/pam.d/system-auth -p rx -k password_policy_discovered</pre> <p>Here,-w stands for the file path monitoring password policy files location, -p stands for permissions and -k is the field which provides a name to the log logged in the Unix. retain the name as "password_policy_discovered", because, we have used the same string name in one of the variable in the rule condition to catch these events.</p> <p>Restart audit service.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p> <p>https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder</p>
Possible Data Exfiltration	<p>Detects suspicious amount of data transferred to any host outside the protect network.</p>
Possible Horizontal Scan Detected	<p>Detects when an adversary scans mutiple target addresses over a victim's firewall. By default, the aggregation is set to 50 hits in 1 minute.</p> <p>Note : A horizontal scan is described as scan against a group of IPs for a single port.</p>
Possible Vertical Scan Detected	<p>Detects adversaries attempting to scan multiple destination ports. By default, the aggregation is set to 20 hits in 1 minute.</p> <p>Note: A vertical scan is described as a single IP being scanned for multiple ports.</p>
Privilege Escalation Attempt Detected	<p>Detects privileged exploit attacks through various ways gathering information from IDS.</p>

Name	Description
Reconnaissance Activity Detected	Detects reconnaissance activity.
Remote System Discovery	<p>Detects adversaries looking for details about other systems by IP address, hostname, or other logical identifiers on a network.</p> <p>Linux Note: To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <pre>-a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve</pre> <p># For monitoring particular file location, we have to add the rule below to the file:</p> <pre>-w /etc/hosts -p rwa -k hosts_file_access</pre> <p>Here, -w stands for the file path monitoring hosts location, -p stands for permissions, and -k is the field which provides a name to the log logged in the Unix. retain the name as "hosts_file_access", because, we have used the same string name in one of the variable in the rule condition to catch these events.</p> <p>Restart audit service.</p> <p>Windows Note: To capture the Windows logs when an adversary tries to open and read certain files or directories, follow instructions provided in the link below.</p> <p>https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder</p>
Scanning IP Blocks	Detects adversary attempting to run scans to gather information that can be used during the MITRE chain. The scope of this rule is only for a possible insider trying to scan IP blocks to target another system.
Suspicious Network Scanning	Detects adversaries attempting to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.
Suspicious Network Sniffing	Detects suspicious network sniffing activities happening on the network.

Name	Description
System Network Configuration Discovery	<p>Detects adversaries looking for details about the network configuration and settings of systems they access.</p> <p>Linux Note: To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <p>-a exit,always -F arch=b64 -F euid=0 -S execve</p> <p>-a exit,always -F arch=b32 -F euid=0 -S execve</p> <p>Restart audit service.</p>
System Network Connections Discovery	<p>Detects adversaries looking for details about the network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.</p> <p>Linux Note: To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine.</p> <p>Path: /etc/audit/audit.rules</p> <p>Include the below rules based on the linux architecture:</p> <p>-a exit,always -F arch=b64 -F euid=0 -S execve</p> <p>-a exit,always -F arch=b32 -F euid=0 -S execve</p> <p>Restart audit service.</p> <p>Windows Note: To capture the Windows logs, enable command line auditing in the below policy location paths.</p> <p>Administrative Templates\System\Audit Process Creation</p> <p>Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Configuration\Detailed Tracking</p> <p>https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing</p> <p>PowerShell Note: To capture the PowerShell logs, make necessary modifications as per the below connector guide link.</p> <p>https://community.microfocus.com/dcvta86296/attachments/dcvta86296/connector-documentation/1290/2/MSPowershellWinEvtLog_N.pdf</p>
Vulnerability Scanning	<p>Detects adversary attempts to run scans to gather the information that can be used during the next stages in the MITRE Chain. The scope of this rule is only for a possible insider trying to do a vulnerability scan to target a victim machine.</p>

Perimeter Monitoring

Name	Description
Egress Communications to Suspicious Country	Detects egress communications to a suspicious country.
Egress Communications with Cleartext Protocol	Detects cleartext protocols crossing a perimeter.
Egress DNS Communications Passed by Firewall	Detects egress DNS communications passed by firewall. This rule is disabled by default, because volume might be very high if asset modeling for DNS servers is not done.
Egress Restricted Services Communications Passed by Firewall	Detects egress communications to restricted services passed by firewall.
High Volume of Denies to Same Destination	Detects high volumes of denials to the same destination.
Tor Traffic Activity Detected On The Network	Detects outbound traffic is detected on ports 9001 or 9030, these ports are used by Tor for network communication.

Vulnerability Monitoring

Name	Description
Attack To Vulnerable Asset	Detects exploitation attempts against a vulnerable asset.

Use Cases

Name	Description	Location
Application Monitoring	Contains resources for application monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/Application Monitoring
Account Activity	Includes different resources to monitor the account activities below. <ul style="list-style-type: none"> • Authentication attempts to disabled account • Privileged account locked out • Members added and removed from privileged groups within 24 hours • User accounts created and deleted within 24 hours 	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Account Activity
Brute Force Attacks	Tracks brute force login attempts and generates alerts for successful brute force attacks.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Brute Force Attacks

Name	Description	Location
Unsuccessful User Logins	Includes different resources to monitor the unsuccessful login activities below. <ul style="list-style-type: none"> • Consecutive Unsuccessful Logins to Administrative Account • Consecutive Unsuccessful Logins to Same Account from different Countries • Consecutive Unsuccessful Logins to Same Account from different IPs • Multiple Failed Login to Different Accounts from Single Source • General Unsuccessful Logins • Failed Login count by user accounts ,source and destination systems 	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Unsuccessful User Logins
Host Monitoring	Contains resources that are included in host monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Host Monitoring
Malware Monitoring	Contains resources that are included in malware monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/Malware Monitoring
Attacks and Suspicious Activity Overview	Includes different resources to monitor attacks and suspicious activity reported by ArcSight Connectors based on ArcSight categorization.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/Attacks and Suspicious Activity Overview
Network Monitoring	Contains resources for network monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/Network Monitoring
Perimeter Monitoring	Focused on events regarding boundary transitions and connections between entities.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/Perimeter Monitoring
Security Threat Monitoring	This is a master use case, and contains multiple child use cases.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring
Vulnerability Monitoring	Contains resources that are included in vulnerability monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/Vulnerability Monitoring

Threat Intelligence Platform Content

This appendix contains individual tables for each Threat Intelligence Platform resource. These tables have been updated to include 4.0 content.

[Active Channel](#)

[Active Lists](#)

[Dashboards](#)

[Data Monitor](#)

[Field Set](#)

[Fields](#)

[Filters](#)

[Integration Commands](#)

[Queries](#)

[Query Viewers](#)

[Rules](#)

[Trends](#)

[Use Case](#)

Active Channel

Name	Description	Location
APT and 0-day Related Activity	Displays all the APT and 0-day related events.	/All Active Channels/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Related Activity

Active Lists

Some active lists require configuration by the customer, these are marked with an asterisk.

Name	Description	Location
APT TMP Tracking	Temporary APT tracking active list used for the APT Tracking active list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/APT TMP Tracking
APT Tracking	Tracks APT-related events based on information from the Threat Intelligence Platform active lists.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/APT Tracking
Internal Address Found in Reputation Data	Stores internal IP addresses found in the reputation list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Internal Address Found in Reputation Data
Internal Domain Found in Suspicious Domains List	Stores internal domains found on the suspicious domain list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Internal Domain Found in Suspicious Domains List
IoC Data Update by Hour	Stores IoC Data that is updated every hour.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/IoC Data Update by Hour
IoC Reputation Data	Stores the intelligence data feeds.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/IoC Reputation Data
Suspicious Addresses List	Contains suspicious addresses collected from GTAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Addresses List
Suspicious Domain List	Contains suspicious domains collected from GTAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List
Suspicious Email List	Contains suspicious emails collected from GTAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email List

Name	Description	Location
Suspicious Hash List	Contains suspicious hash collected from GTAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash List
Suspicious Protocol Tracking	Contains suspicious inbound traffic.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Protocol Tracking
Suspicious URL List	Contains suspicious URLs collected from GTAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL List
Track GTAP Connector	<p>Stores information when the GTAP SmartConnector receives or processes data.</p> <p>By default, the connector downloads data every two hours, as a result, the TTL is 2 hours 5 minutes. If entries are not updated after TTL, meaning something is wrong with connector, a rule will be triggered by audit even from expired entries. If the interval is modified, please change TTL accordingly.</p>	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Track GTAP Connector
Additional Suspicious Addresses*	Define suspicious IP addresses.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious Addresses
Additional Suspicious Domain*	Define suspicious domains.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious Domain
Additional Suspicious Email*	Define suspicious emails.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious Email

Name	Description	Location
Additional Suspicious Hash*	Define suspicious hash.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious Hash
Additional Suspicious URL*	Define suspicious URLs.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious URL
Exception Addresses*	Define IP addresses that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Exception Addresses
Exception Domain*	Define domains that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Exception Domain
Exception Email*	Define emails that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Exception Email
Exception Hash*	Define hash that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Exception Hash
Exception URL*	Define URLs that will NOT be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Exception URL

Dashboards

Name	Description	Location
Data Feed Overview	Displays an overview of your data feed.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview
GTAP Health Status	This dashboard shows the latest status of GTAP Connector. It will appear red if there is no update for certain period of time or if there are error messages from connector. Otherwise, it will show green.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/GTAP Health Status
Threat Intelligence Security Incidents Overview	This dashboard displays overview of threat intelligence alerts.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Security Incidents Overview
TI Confidence Comparison - Open Source vs Galaxy-curated	Displays confidence comparison between CyberRes and open source TI feed. What we can find is that CyberRes Galaxy TI data feed has much more high confidence feeds.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Comparison - Open Source vs Galaxy-curated TI Confidence Details Displays a confidence reputation data overview. /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Details Top Malware and CVE Displays a top malware and CVE. /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware and CVE Top Malware Types Displays reputation data overview by malware type. /All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware Types
TI Confidence Details	Displays a confidence reputation data overview.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Details
Top Malware and CVE	Displays a top malware and CVE.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware and CVE
Top Malware Types	Displays reputation data overview by malware type.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Top Malware Type

Data Monitor

Name	Description	Location
GTAP Connector Status	Shows the latest status of GTAP Connector. It will show red if there is no update for certain time of period or if there are error messages from connector. Otherwise, it will show green.	/All Data Monitors/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Status

Field Set

Name	Description	Location
APT Tracking	Field set for APT Tracking.	/All Field Sets/ArcSight Foundation/Threat Intelligence Platform/APT Tracking

Fields

Fields have individual tables organized by sub folder. All fields function as variables unless otherwise noted.

Common

Name	Description	Location
TMP APT Tracking Active List Columns (getTMPAPTtrackingActiveListColumns)	Returns a list with the columns from the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking Active List Columns
TMP APT Tracking Attacker Address (getTMPAPTtrackingAtkAddress)	Returns the attacker address value from the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking Attacker Address
TMP APT Tracking EventType (getTMPAPTtrackingEventType)	Returns the eventType value from the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking EventType

Name	Description	Location
TMP APT Tracking IndicatorValue (getTMPAPTtrackingIndicatorValue)	Returns the indicatorValue value from the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking IndicatorValue
TMP APT Tracking List Entry (getTMPAPTactiveListEntry)	Returns the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking List Entry
TMP APT Tracking Target Address (getTMPAPTtrackingTgtAddress)	Returns the target address value from the APT TMP Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/_TMP Tracking/TMP APT Tracking Target Address
APT Tracking Active List Columns (getAPTtrackingActiveListColumns)	Returns a list with the columns from the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking Active List Columns
APT Tracking List Entry (getAPTtrackingActiveListEntry)	Returns the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking List Entry
APT Tracking List Entry For Correlation Events (getAPTtrackingActiveListEntryCorrelation)	Returns the APT Tracking active list entries for APT correlation events.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking List Entry For Correlation Events
APT Tracking Attacker Address (getAPTtrackingAtkAddress)	Returns the attacker address value from the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking Attacker Address
APT Tracking Information (getAPTtrackingDescriptionOrInfo)	Returns the extraInfo or description from the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking Information

Name	Description	Location
APT Tracking IndicatorValue (getAPTtrackingIndicatorValue)	Returns the indicatorValue from the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking IndicatorValue
APT Tracking Target Address (getAPTtrackingTgtAddress)	Returns the target address value from the APT Tracking active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/APT Tracking/APT Tracking Target Address
getActiveListColumnsList	Returns a list with the columns from the active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/getActiveListColumnsList
getHighSeverity	Returns the severity for threat level high.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/High/getHighSeverity
getHighPriority (getThreatLevelHighPriority)	Returns the priority for threat level high.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/High/getHighPriority
highThreatLevelMapping	Returns the values from the threat level mapping active list for threat level high.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/High/highThreatLevelMapping
getLowPriority (getThreatLevelLowPriority)	Returns the priority for threat level low.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Low/getLowPriority
getLowSeverity (getThreatLevelLowSeverity)	Returns the severity for threat level low.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Low/getLowSeverity
lowThreatLevelMapping	Returns the values from the threat level mapping active list for threat level low.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Low/lowThreatLevelMapping

Name	Description	Location
getMediumPriority (getThreatLevelMediumPriority)	Returns the priority for threat level medium.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Medium/getMediumPriority
getMediumSeverity (getThreatLevelMediumSeverity)	Returns the severity for threat level medium.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Medium/getMediumSeverity
mediumThreatLevelMapping	Returns the values from the threat level mapping active list for threat level medium.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Medium/mediumThreatLevelMapping
getUndefinedPriority (getThreatLevelUndefinedPriority)	Returns the priority for threat level undefined.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Undefined/getUndefinedPriority
getUndefinedSeverity (getThreatLevelUndefinedSeverity)	Returns the severity for threat level undefined.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Undefined/getUndefinedSeverity
undefinedThreatLevelMapping	Returns the values from the threat level mapping active list for threat level undefined.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Common/Threat Level/Undefined/undefinedThreatLevelMapping

Constants

Name	Description	Location
ADDRESS TYPE (aptTrackingAddressType)	Constant value for address type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/APT Tracking/ADDRESS TYPE
DOMAIN TYPE (aptTrackingDomainType)	Constant value for domain type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/APT Tracking/DOMAIN TYPE
EMAIL TYPE (aptTrackingEmailType)	Constant value for email type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/APT Tracking/EMAIL TYPE

Name	Description	Location
FILE HASH TYPE (aptTrackingFileHashType)	Constant value for file hash type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/APT Tracking/FILE HASH TYPE
URL TYPE (aptTrackingURLType)	Constant value for URL type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/APT Tracking/URL TYPE
HIGH THREAT (HighThreatLevel)	Constant value for threat level high: Sophisticated APT malware or 0-day attack.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/Threat Level/HIGH THREAT
LOW THREAT (LowThreatLevel)	Constant value for threat level low: Mass Malware.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/Threat Level/LOW THREAT
MEDIUM THREAT (MediumThreatLevel)	Constant value for threat level medium: APT Malware	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/Threat Level/MEDIUM THREAT
UNDEFINED THREAT (undefinedThreatLevel)	Constant value for threat level undefined: No Risk	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Constants/Threat Level/UNDEFINED THREAT

Suspicious Address

Name	Description	Location
dstAdditionalAddressEntry	Returns the threat metadata from the Additional Suspicious Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAdditionalAddressEntry
dstAddressIndicatorType	Returns an indicator type for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressIndicatorType
dstAddressIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressIndicatorType1
dstAddressIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressIndicatorType2
dstAddressIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressIndicatorType3

Name	Description	Location
dstAddressIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressIndicatorTypeList
dstAddressPriority	Returns the priority based on the threat level for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressPriority
dstAddressReference	Returns the reference for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressReference
dstAddressSeverity	Returns the severity based on the threat level for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressSeverity
dstAddressThreatLevel	Returns the threat level for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressThreatLevel
dstAddressThreatLevelMapping	Returns the severity and priority based on the threat level for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressThreatLevelMapping
dstAddressValue	Returns addresses for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstAddressValue
dstExceptionAddressEntry	Returns the threat metadata from the Exception Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstExceptionAddressEntry
dstSuspiciousAddressEntry	Returns the threat metadata from the Suspicious Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/dstSuspiciousAddressEntry

Name	Description	Location
srcAdditionalAddressEntry	Returns the threat metadata from the Additional Suspicious Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAdditionalAddressEntry
srcAddressIndicatorType	Returns an indicator type for the Source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressIndicatorType
srcAddressIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressIndicatorType1
srcAddressIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressIndicatorType2
srcAddressIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressIndicatorType3
srcAddressIndicatorTypeList	Returns the list of indicator type separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressIndicatorTypeList
srcAddressPriority	Returns the priority based on the threat level for the source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressPriority
srcAddressSeverity	Returns the severity based on the threat level for the source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressSeverity
srcAddressThreatLevel	Returns the threat level for the source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressThreatLevel

Name	Description	Location
srcAddressThreatLevelMapping	Returns the severity and priority based on the threat level for the source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressThreatLevelMapping
srcAddressValue	Returns addresses for the source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcAddressValue
srcExceptionAddressEntry	Returns the threat metadata from the Exception Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcExceptionAddressEntry
srcSuspiciousAddressEntry	Returns the threat metadata from the Suspicious Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/srcSuspiciousAddressEntry

Suspicious Domain

Name	Description	Location
getDstDomainLevel1	Returns the rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainLevel1
getDstDomainLevel2	Returns the two rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainLevel2
getDstDomainLevel3	Returns the three rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainLevel3
getDstDomainLevel4	Returns the four rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainLevel4
getDstDomainLevel5	Returns the five rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainLevel5

Name	Description	Location
getDstDomainList	Returns the destination domain in list format separated by dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainList
getDstDomainValue	Returns the destination domain (destination fqdn or destination host or request url host).	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getDstDomainValue
getRequestURLDomain	Returns the domain from the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getRequestURLDomain
getSizeOfDstDomainList	Returns the size of the destination domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/getSizeOfDstDomainList
getSizeOfSrcDomainList	Returns the size of the source domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSizeOfSrcDomainList
getSrcDomainLevel1	Returns the rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainLevel1
getSrcDomainLevel2	Returns the two rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainLevel2
getSrcDomainLevel3	Returns the three rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainLevel3
getSrcDomainLevel4	Returns the four rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainLevel4
getSrcDomainLevel5	Returns the five rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainLevel5
getSrcDomainList	Returns the source domain in list format separated by dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainList
getSrcDomainValue	Returns the destination domain (destination fqdn or destination host or request URL host).	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/getSrcDomainValue

Name	Description	Location
dstAdditionalDomainEntry	Returns the threat metadata from the Additional Suspicious Domain List based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstAdditionalDomainEntry
dstAdditionalDomainLevel2	Returns the threat metadata defined by user from Additional Suspicious Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstAdditionalDomainLevel2
dstAdditionalDomainLevel3	Returns the threat metadata defined by user from Additional Suspicious Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstAdditionalDomainLevel3
dstAdditionalDomainLevel4	Returns the four rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstAdditionalDomainLevel4
dstAdditionalDomainLevel5	Returns the five rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstAdditionalDomainLevel5
dstDomainIndicatorType	Returns the source domain in list format separated by dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainIndicatorType
dstDomainIndicatorType1	Returns the destination domain (destination fqdn or destination host or request URL host).	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainIndicatorType1
dstDomainIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainIndicatorType2
dstDomainIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainIndicatorType3
dstDomainIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainIndicatorTypeList
dstDomainPriority	Returns the priority based on threat level for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainPriority

Name	Description	Location
dstDomainReference	Returns the reference for the destination domain either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainReference
dstDomainSeverity	Returns the severity based on threat level for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainSeverity
dstDomainThreatLevel	Returns the threat level for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainThreatLevel
dstDomainThreatLevelMapping	Returns the severity and priority based on threat level for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainThreatLevelMapping
dstDomainValue	Returns domains for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstDomainValue
dstExceptionDomainEntry	Returns the threat metadata from the Exception Domain List based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstExceptionDomainEntry
dstExceptionDomainLevel2	Returns exception domains from Exceptions Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstExceptionDomainLevel2
dstExceptionDomainLevel3	Returns exception domains from Exceptions Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstExceptionDomainLevel3
dstExceptionDomainLevel4	Returns exception domains from Exceptions Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstExceptionDomainLevel4

Name	Description	Location
dstExceptionDomainLevel5	Returns exception domains from Exceptions Domain active list corresponding to the destination domain level 5.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstExceptionDomainLevel5
dstSuspiciousDomainEntry	Returns the the threat metadata from the Suspicious Domain List based on a destination fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstSuspiciousDomainEntry
dstSuspiciousListDomainLevel2	Returns the the threat metadata from Suspicious Domain List corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstSuspiciousListDomainLevel2
dstSuspiciousListDomainLevel3	Returns the threat metadata from Suspicious Domain List corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstSuspiciousListDomainLevel3
dstSuspiciousListDomainLevel4	Returns the suspicious domains from Exceptions Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstSuspiciousListDomainLevel4
dstSuspiciousListDomainLevel5	Returns the threat metadata from Suspicious Domain List corresponding to the destination domain level 5.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/dstSuspiciousListDomainLevel5
srcAdditionalDomainEntry	Returns the entry of a source in the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcAdditionalDomainEntry
srcAdditionalDomainLevel2	Returns additional domain from Additional Suspicious Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcAdditionalDomainLevel2
srcAdditionalDomainLevel3	Returns additional domain from Additional Suspicious Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcAdditionalDomainLevel3
srcAdditionalDomainLevel4	Returns additional domain from Additional Suspicious Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcAdditionalDomainLevel4

Name	Description	Location
srcAdditionalDomainLevel5	Returns additional domain from Additional Suspicious Domain active list corresponding to the source domain level 5.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcAdditionalDomainLevel5
srcDomainIndicatorType	Global variable that displays domain indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainIndicatorType
srcDomainIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainIndicatorType1
srcDomainIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainIndicatorType2
srcDomainIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainIndicatorType3
srcDomainIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainIndicatorTypeList
srcDomainPriority	Returns the priority based on threat level for the source domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainPriority
srcDomainSeverity	Returns the severity based on threat level for the source domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainSeverity
srcDomainThreatLevel	Returns the threat level for the source domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainThreatLevel
srcDomainThreatLevelMapping	Returns the severity and priority based on threat level for the source domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainThreatLevelMapping

Name	Description	Location
srcDomainValue	Returns the domain for the source domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcDomainValue
srcExceptionDomainEntry	Returns the exception domains from the Exceptions - Domain active list based on a source fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcExceptionDomainEntry
srcExceptionDomainLevel2	Returns the exception domains from Exceptions - Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcExceptionDomainLevel2
srcExceptionDomainLevel3	Returns the exception domains from Exceptions - Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcExceptionDomainLevel3
srcExceptionDomainLevel4	Returns the exception domains from Exceptions - Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcExceptionDomainLevel4
srcExceptionDomainLevel5	Returns the exception domain from Exceptions - Domain active list corresponding to the source domain level 5.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel2
srcSuspiciousDomainEntry	Returns the threat metadata from the Suspicious Domain List based on a source fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel2
srcSuspiciousListDomainLevel2	Returns the threat metadata from Suspicious Domain List corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel3

Name	Description	Location
srcSuspiciousListDomainLevel3	Returns the threat metadata from Suspicious Domain List corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel4
srcSuspiciousListDomainLevel4	Returns the threat metadata from Suspicious Domain List corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel5
srcSuspiciousListDomainLevel5	Returns the threat metadata from Suspicious Domain List corresponding to the source domain level 5.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/srcSuspiciousListDomainLevel5

Suspicious Email

Name	Description	Location
dstAdditionalEmailEntry	Returns the entry of the destination username in the Additional Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstAdditionalEmailEntry
dstEmailIndicatorType	Global variable that displays Email Indicator Types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailIndicatorType
dstEmailIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailIndicatorType1
dstEmailIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailIndicatorType2
dstEmailIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailIndicatorType3
dstEmailIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailIndicatorTypeList

Name	Description	Location
dstEmailPriority	Returns the priority based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailPriority
dstEmailSeverity	Returns the severity based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailSeverity
dstEmailThreatLevel	Returns the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailThreatLevel
dstEmailThreatLevelMapping	Returns the severity and priority based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstEmailThreatLevelMapping
dstSuspiciousEmailEntry	Returns the entry of the destination username in the Suspicious Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/dstSuspiciousEmailEntry
srcAdditionalEmailEntry	Returns the entry of a source in the Additional Suspicious Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcAdditionalEmailEntry
srcEmailIndicatorType	Global variable that displays Email Indicator Types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailIndicatorType
srcEmailIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailIndicatorType1
srcEmailIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailIndicatorType2
srcEmailIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailIndicatorType3

Name	Description	Location
srcEmailIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailIndicatorTypeList
srcEmailPriority	Returns the priority based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailPriority
srcEmailSeverity	Returns the severity based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailSeverity
srcEmailThreatLevel	Returns the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailThreatLevel
srcEmailThreatLevelMapping	Returns the severity and priority based on the threat level either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailThreatLevelMapping
srcEmailValue	Returns emails either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcEmailValue
srcSuspiciousEmailEntry	Returns the entry of a source in the Suspicious Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/srcSuspiciousEmailEntry

Suspicious Hash

Name	Description	Location
additionalFileHashEntry	Returns the threat metadata from the Additional Suspicious Hash based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/additionalFileHashEntry
exceptionFileHashEntry	Returns the threat metadata from the Exception Hash based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/exceptionFileHashEntry

Name	Description	Location
getHashValue	Returns the hash value from fields - File Hash and Old File Hash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/getHashValue
hashIndicatorType	Global variable that displays hash indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/hashIndicatorType
hashIndicatorType1	Returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/hashIndicatorType1
hashIndicatorType2	Returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/hashIndicatorType2
hashIndicatorType3	Returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/hashIndicatorType3
hashIndicatorTypeList	Returns the list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/hashIndicatorTypeList
suspiciousFileHashEntry	Returns the threat metadata from the Suspicious Hash List based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/suspiciousFileHashEntry
suspiciousFileHashPriority	Returns the priority based on the threat level either from the Suspicious Hash List active list or the Additional Suspicious Hash active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/suspiciousFileHashPriority

Name	Description	Location
suspiciousFileHashSeverity	Returns the severity based on the threat level either from the Suspicious Hash List active list or the Additional Suspicious Hash active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/suspiciousFileHashSeverity
suspiciousFileHashThreatLevel	Returns the threat level either from the Suspicious Hash List active list or the Additional Suspicious Hash active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/suspiciousFileHashThreatLevel
suspiciousFileHashThreatLevelMapping	Returns the severity and priority based on the threat level either from the Suspicious Hash List active list or the Additional Suspicious Hash active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/suspiciousFileHashThreatLevelMapping

Suspicious URL

Name	Description	Location
additionalUrlEntry	Returns the threat metadata from the Additional Suspicious URL active list based on the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/additionalUrlEntry
exceptionUrlEntry	Returns the threat metadata from the Exception Suspicious URL active list based on the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/exceptionUrlEntry
getUrlValue	Returns the field request URL in lowercase.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/getUrlValue
suspiciousUrlEntry	Returns the threat metadata from the Suspicious URL List based on the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/suspiciousUrlEntry
suspiciousURLPriority	Returns the priority based on the threat level either from the Suspicious URL List active list or the Additional Suspicious URL active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/suspiciousURLPriority

Name	Description	Location
suspiciousURLSeverity	Returns the severity based on the threat level either from the Suspicious URL List active list or the Additional Suspicious URL active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/suspiciousURLSeverity
suspiciousURLThreatLevel	Returns the threat level either from the Suspicious URL List active list or the Additional Suspicious URL active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/suspiciousURLThreatLevel
suspiciousURLThreatLevelMapping	Returns the severity and priority based on the threat level either from the Suspicious URL List active list or the Additional Suspicious URL active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL/suspiciousURLThreatLevelMapping

Filters

Name	Description	Location
APT Correlation Events	Returns all APT correlation events.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT Correlation Events
APT TMP Tracking Events	Returns events related to the APT TMP Tracking active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT TMP Tracking Events
APT Tracking Events	Returns events related to the APT Tracking active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/APT Tracking/APT Tracking Events
Destination in Suspicious Address List APT Malware Related	Identifies the destination address in the Suspicious Addresses active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Destination in Suspicious Address List APT Malware Related
Destination in Suspicious Address List Sophisticated APT Malware or 0-day Related	Identifies the destination address in the Suspicious Addresses active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Destination in Suspicious Address List Sophisticated APT Malware or 0-day Related
Source in Suspicious Address List APT Malware Related	Identifies the source address in the Suspicious Addresses active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Source in Suspicious Address List APT Malware Related

Name	Description	Location
Source in Suspicious Address List Sophisticated APT Malware or 0-day Related	Identifies the source address in the Suspicious Addresses active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Address/Source in Suspicious Address List Sophisticated APT Malware or 0-day Related
Destination in Suspicious Domain List APT Malware Related	Identifies the destination domain in the Suspicious Domain active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Destination in Suspicious Domain List APT Malware Related
Destination in Suspicious Domain List Sophisticated APT Malware or 0-day Related	Identifies the destination domain in the Suspicious Domain active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Destination in Suspicious Domain List Sophisticated APT Malware or 0-day Related
Source in Suspicious Domain List APT Malware Related	Identifies the source domain in the Suspicious Domain active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Source in Suspicious Domain List APT Malware Related
Source in Suspicious Domain List Sophisticated APT Malware or 0-day Related	Identifies the source domain in the Suspicious Domain active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Domain/Source in Suspicious Domain List Sophisticated APT Malware or 0-day Related
Destination in Suspicious Email List APT Malware Related	Identifies the destination username (email address) in the Suspicious Email active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Destination in Suspicious Email List APT Malware Related
Destination in Suspicious Email List Sophisticated APT Malware or 0-day Related	Identifies the destination username (email address) in the Suspicious Email active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Destination in Suspicious Email List Sophisticated APT Malware or 0-day Related
Source in Suspicious Email List APT Malware Related	Identifies the source username (email address) in the Suspicious Email active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Source in Suspicious Email List APT Malware Related
Source in Suspicious Email List Sophisticated APT Malware or 0-day Related	Identifies the source username (email address) in the Suspicious Email active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Email/Source in Suspicious Email List Sophisticated APT Malware or 0-day Related

Name	Description	Location
File Hash in Suspicious Hash List APT Malware Related	Identifies the file hash in the Suspicious Hash active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Hash/File Hash in Suspicious Hash List APT Malware Related
File Hash in Suspicious Hash List Sophisticated APT Malware or 0-day Related	Identifies the file hash in the Suspicious Hash active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious Hash/File Hash in Suspicious Hash List Sophisticated APT Malware or 0-day Related
URL in Suspicious URL List APT Malware Related	Identifies the URL in the Suspicious URL active list where the threat level is medium (APT malware).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious URL/URL in Suspicious URL List APT Malware Related
URL in Suspicious URL List Sophisticated APT Malware or 0-day	Identifies the URL in the Suspicious URL active list where the threat level is high (sophisticated APT malware or 0-day).	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Suspicious URL/URL in Suspicious URL List Sophisticated APT Malware or 0-day
All Sophisticated APT Malware or 0-day Related (Threat Level High)	Returns all events with threat level high: Sophisticated APT malware or 0-day Related.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/All Sophisticated APT Malware or 0-day Related
All APT Malware Related (Threat Level Medium)	Returns all events with threat level medium: APT Malware Related.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/All APT Malware Related
C2 Inbound Communication from a Suspicious Address	Contains correlated events of Command and Control Inbound communication from a Suspicious Address.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Address
C2 Inbound Communication from a Suspicious Domain	Contains correlated events of Command and Control Inbound communication from a Suspicious Domain.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/C2 Inbound Communication from a Suspicious Domain
Destination in Suspicious Address List	Identifies the destination address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Address List
Destination in Suspicious Domain	Detects all events which destination is in the suspicious or additional domain list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain
Destination in Suspicious Domain List	Identifies the destination domain in the Suspicious Domain List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Domain List

Name	Description	Location
Destination in Suspicious Email List	Identifies the destination email address in the Suspicious Email List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Destination in Suspicious Email List
File Hash in Suspicious Hash List	Identifies the file hash in the Suspicious Hash List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/File Hash in Suspicious Hash List
Update events from GTAP Connector	Selects updated events from GTAP Connector.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Health/Update events from GTAP Connector
Source in Suspicious Address List	Identifies the source address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Source in Suspicious Address List
Source in Suspicious Domain List	Identifies the source domain in the Suspicious Domain List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Source in Suspicious Domain List
Source in Suspicious Email List	Identifies the source email address in the Suspicious Email List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Source in Suspicious Email List
URL in Suspicious URL List	Identifies the URL in the Suspicious URL List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/URL in Suspicious URL List

Integration Commands

Name	Description	Location
MISP CIRCL Lookup	Looks for more detailed information on MISP CIRCL. You need to request access which can be done here: https://www.circl.lu/services/misp-malware-information-sharing-platform/#how-to-request-access	/All Integration Commands/ArcSight Foundation/Threat Intelligence Platform/MISP CIRCL Lookup
VirusTotal Hash Lookup	Looks for hash details using VirusTotal.	/All Integration Commands/ArcSight Foundation/Threat Intelligence Platform/VirusTotal Hash Lookup
MISP CIRCL Lookup	Configures the MISP CIRCL lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/Threat Intelligence Platform/MISP CIRCL Lookup
VirusTotal Hash Lookup	Configures the VirusTotal Hash lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/Threat Intelligence Platform/VirusTotal Hash Lookup

Queries

Name	Description	Location
CyberRes-curated Threat Intelligence Feed	Selects data feed counts grouped by confidence in which the creator organization is CyberRes Galaxy.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/CyberRes-curated Threat Intelligence Feed
Data Feed Overview by Confidence	Selects data feed counts grouped by confidence.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Data Feed Overview by Confidence
High Confidence CyberRes-curated Threat Intelligence Feed	Selects data feed counts grouped by confidence in which the creator organization is CyberRes Galaxy.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/High Confidence CyberRes-curated Threat Intelligence Feed
High Confidence Open Source Threat Intelligence provided by MISP CIRCL	Selects data feed counts grouped by high confidence in which the creator organization is open source threat intelligence provided by MISP CIRCL.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/High Confidence Open Source Threat Intelligence provided by MISP CIRCL
Open Source Threat Intelligence provided by MISP CIRCL	Selects data feed counts grouped by confidence which creator org is from open source threat intelligence provided by MISP CIRCL.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Open Source Threat Intelligence provided by MISP CIRCL
Overall Confidence Details	Selects overall confidence details.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Overall Confidence Details
Overview by High Confidence	Selects overall TI data feed by high confidence.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Overview by High Confidence
Overview by Low Confidence	Selects overall TI data feed by low confidence.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Overview by Low Confidence
Overview by Medium Confidence	Selects overall TI data feed by medium confidence.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Overview by Medium Confidence
Suspicious Address by Confidence	Selects confidence and counts from the suspicious address list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Suspicious Address by Confidence
Suspicious Domain by Confidence	Selects confidence and counts from the suspicious domain list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Suspicious Domain by Confidence

Name	Description	Location
Suspicious Hash by Confidence	Selects confidence and counts from the suspicious hash list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Suspicious Hash by Confidence
Suspicious URL by Confidence	Selects confidence and counts from the suspicious URL list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/Suspicious URL by Confidence
Data Feed of Suspicious Address	Selects data feed of suspicious addresses.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed of Suspicious Address
Data Feed of Suspicious Domain	Selects data feed of suspicious domains.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed of Suspicious Domain
Data Feed of Suspicious Emails	Selects data feed of suspicious emails.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed of Suspicious Emails
Data Feed of Suspicious Hash	Selects data feed of suspicious hash.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed of Suspicious Hash
Data Feed of Suspicious URL	Selects data feed of suspicious URLs.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed of Suspicious
URL Data Feed Overview by CreatorOrg	Selects data feed grouped by the creator organization.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed Overview by CreatorOrg
Data Feed Overview by Type	Selects data feed by type.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed Overview by Type
IoC Data Update by Hour	Selects IoC data update by hour.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/IoC Data Update by Hour
Most Active Threat Actors	Selects most active actors.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Most Active Threat Actors
Data Feed Overview by Indicator Type	Selects data feed overview by malware type.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Data Feed Overview by Indicator Type
Suspicious Address by Indicator Type	Selects indicator type and counts from suspicious address list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Suspicious Address by Indicator Type

Name	Description	Location
Suspicious Domain by Indicator Type	Selects indicator type and counts from suspicious domain list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Suspicious Domain by Indicator Type
Suspicious Hash by Indicator Type	Selects indicator type and counts from suspicious hash list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Suspicious Hash by Indicator Type
Suspicious URL by Indicator Type	Selects indicator type and counts from suspicious url list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Suspicious URL by Indicator Type
Data Feed Overview by AV Signature	Selects data feed by av signatures.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Data Feed Overview by AV Signature
Data Feed Overview by CVE	Selects data feed by CVE.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Data Feed Overview by CVE
Data Feed Overview by Malware Name	Selects data feed by malware name.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Data Feed Overview by Malware Name
Data Feed Overview by Malware Type	Selects data feed by malware types.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Data Feed Overview by Malware Type
Malware and AV Details	Selects malware and av details.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Malware and AV Details
Threat Intelligence Alerts by Date	Selects threat intelligence platform alerts by date.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Alerts by Date
Threat Intelligence Alerts by Type	Selects rule group names detected by threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Alerts by Type
Threat Intelligence Alerts Details	Selects alert details detected by threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Alerts Details
Top Alerts by Attacker	Selects attacker addresses detected by threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Top Alerts by Attacker
Top Alerts by Target	Selects target addresses detected by threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Top Alerts by Target

Query Viewers

Name	Description	Location
Actionable IoC's from Galaxy-curated TI Feed	Displays high confidence Galaxy-curated TI feed.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Actionable IoC's from Galaxy-curated TI Feed
Actionable IoC's from Open Source (MISP CIRCL) TI Feed	Displays high confidence open source (MISP CIRCL) TI feed.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Actionable IoC's from Open Source (MISP CIRCL) TI Feed
Confidence in Suspicious Address	Displays top confidence entries from the Suspicious Address list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Confidence in Suspicious Address
Confidence in Suspicious Domain	Displays top confidence entries from the Suspicious Domain list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Confidence in Suspicious Domain
Confidence in Suspicious Hash	Displays top confidence entries from the Suspicious Hash list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Confidence in Suspicious Hash
Confidence in Suspicious URL	Displays top confidence entries from the Suspicious URL list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Confidence in Suspicious URL
CyberRes Galaxy-curated Threat Intelligence Feed	Displays data feed overview grouped by confidence in which the creator organization is CyberRes Galaxy.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/CyberRes Galaxy-curated Threat Intelligence Feed
Data Feed Overview by Confidence	Displays data feed overview by confidence.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Data Feed Overview by Confidence
Data Feed Overview by High Confidence	Displays data feed overview by high confidence.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Data Feed Overview by High Confidence


Name	Description	Location
Data Feed Overview by Low Confidence	Displays data feed overview by low confidence.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Data Feed Overview by Low Confidence Data Feed
Overview by Medium Confidence	Displays data feed overview by medium confidence.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Data Feed
Overview by Medium Confidence Open Source (MISP CIRCL) Threat Intelligence	Displays data feed counts grouped by confidence in which the creator organization is from open source threat intelligence provided by MISP CIRCL.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Open Source (MISP CIRCL) Threat Intelligence
Overall Confidence Details	Displays overall confidence details.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Overall Confidence Details
Data Feed Overview by Attribute Type	Displays the data feed overview by attribute type.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Data Feed Overview by Attribute Type
IoC Data Update by Hour	Displays IoC data update by hour.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/IoC Data Update by Hour
Most Active Threat Actors	Displays most active actors.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Most Active Threat Actors
Top Data Feed Overview by CreatorOrg	Displays the data feed overview by CreatorOrg.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Top Data Feed Overview by CreatorOrg
Last 20 Threat Intelligence Alerts	Displays the last 20 threat intelligence alerts.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Last 20 Threat Intelligence Alerts
Malware and AV Details	Displays malware and AV details.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Malware and AV Details

Name	Description	Location
Top Data Feed Overview by AV Signature	Displays top data feed overview by AV signature.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Top Data Feed Overview by AV Signature
Top Data Feed Overview by CVE	Displays top data feed overview by CVE.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Top Data Feed Overview by CVE
Top Data Feed Overview by Malware Name	Displays data feed overview by malware name	. /All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Top Data Feed Overview by Malware Name
Top Data Feed Overview by Malware Type	Displays data feed overview by malware name.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Top Data Feed Overview by Malware Type
Top Data Feed Overview by Malware Type	Displays data feed overview by malware name.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware Type/Top Data Feed Overview by Malware Type
Top Malware Type in Suspicious Address	Displays top indicator types from the Suspicious Address list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware Type/Top Malware Type in Suspicious Address
Top Malware Type in Suspicious Domain	Displays top indicator types from the Suspicious Domain list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware Type/Top Malware Type in Suspicious Domain
Top Malware Type in Suspicious Hash	Displays top indicator types from the Suspicious Hash list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware Type/Top Malware Type in Suspicious Hash
Top Malware Type in Suspicious URL	Displays top indicator types from the Suspicious URL list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware Type/Top Malware Type in Suspicious URL
Threat Intelligence Alerts Details	Displays threat intelligence alerts details.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Alerts Details

Name	Description	Location
Threat Intelligence Alerts Details 7 Days	Displays threat intelligence alerts details for the last seven days.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Alerts Details 7 Days
Threat Intelligence Security Incidents by Type	Displays threat intelligence alerts by type.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Security Incidents by Type
Threat Intelligence Security Incidents per Day	Displays alerts per day.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Security Incidents per Day
Top Threat Intelligence Security Incidents by Attacker	Displays top alerts by attacker address.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Top Threat Intelligence Security Incidents by Attacker
Top Threat Intelligence Security Incidents by Target	Displays top alerts by target address.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Top Threat Intelligence Security Incidents by Target

Rules

Rules have individual tables organized by sub folder.

 **Note:** To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

APT and 0-day Activity

Name	Description	Location
Add Additional Address To APT Tracking List	Adds additional addresses to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Additional Address To APT Tracking List
Add Additional Domain To APT Tracking List	Adds additional domains to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Additional Domain To APT Tracking List

Appendices

Name	Description	Location
Add Additional Email To APT Tracking List	Adds additional email addresses to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Additional Email To APT Tracking List
Add Additional File Hash To APT Tracking List	Adds the additional file hash to the APT Tracking list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Additional File Hash To APT Tracking List
Add Additional URL To APT Tracking List	Adds additional URLs to the APT Tracking list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Additional URL To APT Tracking List
Add Suspicious Addresses To APT Tracking List	Adds suspicious addresses to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Suspicious Addresses To APT Tracking List
Add Suspicious Domain To APT Tracking List	Adds suspicious domains to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Suspicious Domain To APT Tracking List
Add Suspicious Email To APT Tracking List	Adds suspicious email addresses to the APT Tracking List.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Suspicious Email To APT Tracking List
Add Suspicious File Hash To APT Tracking List	Adds suspicious file hash to the APT Tracking list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Suspicious File Hash To APT Tracking List
Add Suspicious URL To APT Tracking List	Adds suspicious URLs to the APT Tracking list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/APT Tracking/Add Suspicious URL To APT Tracking List
Possible 0-day Related Activity	Detects when APT related indicators are added to the APT Tracking active list and the threat level is high (Sophisticate APT Malware or 0-day) and 0-day, Oday or zero day is the indicatorType.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Possible 0-day Related Activity
Address is related to APT Malware Activity	Detects when the source or destination address is in the (additional) suspicious address active list with threat level medium (APT malware).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Address/Address is related to APT Malware Activity

Name	Description	Location
Address is related to Sophisticated APT Malware or 0-day Activity	Detects when the source or destination address is in the (additional) suspicious address active list with threat level high (Sophisticated APT malware or 0-day Activity).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Address/Address is related to Sophisticated APT Malware or 0-day Activity
Domain is related to APT Malware Activity	Detects when the domain is in the (additional) suspicious domain active list with threat level medium (APT malware).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Domain/Domain is related to APT Malware Activity
Domain is related to Sophisticated APT malware or 0-day Activity	Detects when the domain is in the is in the (additional) suspicious address active list with threat level high (Sophisticated APT malware or 0-day Activity).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Domain/Domain is related to Sophisticated APT malware or 0-day Activity
Email Address is related to APT Malware Activity	Detects when the email address is in the (additional) suspicious email active list with threat level medium (APT malware).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Email/Email Address is related to APT Malware Activity
Email Address is related to Sophisticated APT malware or 0-day Activity	Detects when the email address is in the (additional) suspicious email active list with threat level high (Sophisticated APT malware or 0-day Activity).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious Email/Email Address is related to Sophisticated APT malware or 0-day Activity
File Hash is related to APT Malware Activity	Detects when the file hash is in the (additional) suspicious hash active list with threat level medium (APT malware).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious File Hash/File Hash is related to APT Malware Activity

Name	Description	Location
File Hash is related to Sophisticated APT malware or 0-day Activity	Detects when the file hash is in the (additional) suspicious hash active list with threat level high (Sophisticated APT malware or 0-day Activity).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious File Hash/File Hash is related to Sophisticated APT malware or 0-day Activity
URL is related to APT Malware Activity	Detects when the URL is in the (additional) suspicious URL active list with threat level medium (APT malware).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious URL/URL is related to APT Malware Activity
URL is related to Sophisticated APT malware or 0-day Activity	Detects when the URL is in the (additional) suspicious URL active list with threat level high (Sophisticated APT malware or 0-day Activity).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/APT and 0-day Activity/Suspicious URL/URL is related to Sophisticated APT malware or 0-day Activity

Botnet Activity

Name	Description	Location
Command and Control Communication to a Suspicious Address	Detects outbound traffic to suspicious command and control server.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Address
Command and Control Communication to a Suspicious Domain	Detects outbound traffic to suspicious command and control domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Communication to a Suspicious Domain
Command and Control Inbound Communication on Commonly Used Port	Detects Inbound C2 communications over Commonly used port to bypass proxies and firewalls that have been improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Inbound Communication on Commonly Used Port
Command and Control Inbound Communication on Uncommonly Used Port	Detects Inbound C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Inbound Communication on Uncommonly Used Port

Name	Description	Location
Command and Control Multiband Communication	<p>Detects split communications between different protocols. There could be one protocol for inbound command and control and another for outbound data, allowing it to bypass certain firewall restrictions. The split could also be random to simply avoid data threshold alerts on any one communication.</p> <p>This rule is dependent on the rule /All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Inbound Suspicious Traffic.</p>	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Multiband Communication
Command and Control Outbound Communication on Commonly Used Port	Detects Outbound C2 communications over a Commonly used port to bypass proxies and firewalls that have been improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Outbound Communication on Commonly Used Port
Command and Control Outbound Communication on Uncommonly Used Port	Detects Outbound C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Outbound Communication on Uncommonly Used Port
Command and Control Remote File Copy	Detects files copied from an external adversary-controlled system through the Command and Control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Remote File Copy
Data Transfer over Alternative Protocol to C2 Server	Creates a correlation event when there is communication to a command and control server over alternative protocol.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Data Transfer over Alternative Protocol to C2 Server

Name	Description	Location
Data Transfer over Main Channel to C2 Server	Creates a correlation event when there is communication to a command and control server over main channel.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Data Transfer over Main Channel to C2 Server
Inbound Suspicious Traffic	Lightweight rule that captures inbound traffic from a suspicious address into an active list called Suspicious Protocol Tracking. Then it is used by the rule /All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Command and Control Multiband Communication.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Inbound Suspicious Traffic
Potential Information Transfer Through Removable Media Over C2 Communication	Detects potential information transfers to removable media over command and control server.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Potential Information Transfer Through Removable Media Over C2 Communication

Dangerous Browsing

Name	Description	Location
Dangerous Browsing to a Suspicious Address	Detects outbound web traffic to a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Dangerous Browsing to a Suspicious Address
Dangerous Browsing to a Suspicious Domain	Detects outbound web traffic to a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Dangerous Browsing to a Suspicious Domain
Dangerous Browsing to a Suspicious URL	Detects outbound traffic with suspicious URLs.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Dangerous Browsing to a Suspicious URL

GTAP Connector Health

Name	Description	Location
Error in GTAP Connector Service Message	Detects GTAP Connector errors receiving or processing a malicious list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Health/Error in GTAP Connector Service Message
No Update from GTAP Connector	Detects if any entries expire from the Track GTAP Connector list, meaning there is no update from connector for a certain time period (defined by active list TTL).	/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Health/No Update from GTAP Connector

Name	Description	Location
Track GTAP Connector Service Message	Tracks GTAP Connector service message events and adds them to an active list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Health/Track GTAP Connector Service Message
Track GTAP Connector Update Count	Tracks GTAP connector update counts and sends them to an active list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/GTAP Connector Health/Track GTAP Connector Update Count

High Confidence Alerts

Name	Description	Location
High Confidence Alerts to Suspicious Source	Detects outbound suspicious traffic with high or very high confidence.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/High Confidence Alerts to Suspicious Source
High Confidence Alerts with Suspicious File Hash	Detects alerts of suspicious file hash with high or very high confidence.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/High Confidence Alerts/High Confidence Alerts with Suspicious File Hash

Internal Asset Found in Reputation List

Name	Description	Location
Internal Destination Address Found in Suspicious Address List	Detects internal destination addresses found on the Suspicious Address list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/Internal Destination Address Found in Suspicious Address List
Internal Destination Domain Found in Suspicious Domain List	Detects internal destination domains found on the Suspicious Domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/Internal Destination Domain Found in Suspicious Domain List
Internal Source Address Found in Suspicious Address List	Detects internal source addresses found on the Suspicious Address list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/Internal Source Address Found in Suspicious Address List
Internal Source Domain Found in Suspicious Domain List	Detects internal source domains found on the Suspicious Domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/Internal Source Domain Found in Suspicious Domain List

Malware

Name	Description	Location
Malware Activity to a Suspicious Address	Detects outbound traffic to a suspicious malware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/Malware Activity to a Suspicious Address
Malware Activity to a Suspicious Domain	Detects outbound traffic to a suspicious malware domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/Malware Activity to a Suspicious Domain

Phishing

Name	Description	Location
Outbound Communication to a Phishing Address	Detects outbound traffic to suspicious phishing address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Phishing/Outbound Communication to a Phishing Address
Outbound Communication to a Phishing Domain	Detects outbound traffic to suspicious phishing domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Phishing/Outbound Communication to a Phishing Domain

Ransomware

Name	Description	Location
Ransomware Activity to a Suspicious Address	Detects outbound traffic to a suspicious ransomware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Ransomware/Ransomware Activity to a Suspicious Address
Ransomware Activity to a Suspicious Domain	Detects outbound traffic to a suspicious ransomware domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Ransomware/Ransomware Activity to a Suspicious Domain

Suspicious Activity

Name	Description	Location
Add Indicator Types	Adds indicator types to a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Add Indicator Types
Inbound Traffic from a Suspicious Address	Detects inbound traffic from a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Inbound Traffic from a Suspicious Address
Inbound Traffic from a Suspicious Domain	Detects inbound traffic from a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Inbound Traffic from a Suspicious Domain

Name	Description	Location
Outbound Traffic to a Suspicious Address	Detects outbound traffic to a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Outbound Traffic to a Suspicious Address
Outbound Traffic to a Suspicious Domain	Detects outbound traffic to a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Outbound Traffic to a Suspicious Domain
Remove Indicator Types	Removes indicator type from a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/Remove Indicator Types

Suspicious DNS Query

Name	Description	Location
DNS Query to a Suspicious Address	Detects outbound suspicious DNS queries to suspicious addresses.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious DNS Query/DNS Query to a Suspicious Address
DNS Query to a Suspicious Domain	Detects outbound suspicious DNS queries to suspicious domains.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious DNS Query/DNS Query to a Suspicious Domain

Suspicious Email

Name	Description	Location
Email Received From Suspicious Address	Detects emails received from a suspicious address and when the indicator type is not listed on the active list: Indicator Types.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Email Received From Suspicious Address
Email Sent To Suspicious Address	Detects emails sent to suspicious receiver.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Email Sent To Suspicious Address
Received Email From A Command And Control Address	Detects emails received from a command and control address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Received Email From A Command And Control Address
Received Email From Malware Address	Detects emails received from a malware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Received Email From Malware Address

Name	Description	Location
Received Email From Phishing Address	Detects emails received from a phishing address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Received Email From Phishing Address
Received Email From Ransomware Address	Detects emails received from a ransomware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Received Email From Ransomware Address
Received Phishing Email With An Attachment	Detects emails received containing attachment from suspicious source.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/Received Phishing Email With An Attachment

Suspicious File Hash

Name	Description	Location
Suspicious File Hash Activity in Host	Detects suspicious file hash on hosts.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious File Hash/Suspicious File Hash Activity in Host

Trends

Name	Description	Location
Summary of Suspicious Addresses	Stores the summary of suspicious addresses.	/All Trends/ArcSight Foundation/Threat Intelligence Platform/Summary of Suspicious Addresses
Summary of Suspicious Domains	Stores the summary of suspicious domains.	/All Trends/ArcSight Foundation/Threat Intelligence Platform/Summary of Suspicious Domains
Summary of Suspicious Emails	Stores the summary of suspicious emails.	/All Trends/ArcSight Foundation/Threat Intelligence Platform/Summary of Suspicious Emails
Summary of Suspicious Hashes	Stores the summary of suspicious hashes.	/All Trends/ArcSight Foundation/Threat Intelligence Platform/Summary of Suspicious Hashes
Summary of Suspicious URL	Stores the summary of suspicious URLs.	/All Trends/ArcSight Foundation/Threat Intelligence Platform/Summary of Suspicious URL

Use Case

Name	Description	Location
Threat Intelligence Platform	Detects threats based on intelligence data collected from MISP.	/All Use Cases/ArcSight Foundation/Threat Intelligence Platform/Threat Intelligence Platform

Publication Status

Released: March 23, 2023

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 ArcSight Administration and ArcSight System Standard Content Guide (ESM 7.6.4)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!