opentext™

ArcSight Detect

Software Version: 8.1.0

ArcSight Administration and ArcSight System Standard Content Guide

Document Release Date: October 2023
Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

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?

Standard content is a series of coordinated resources, such as dashboards, active channels, filters, rules, and so on that is designed to give you pre-installed comprehensive correlation, monitoring, and alerting 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 the the ArcSight Administration content package. This package is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components. You can view the list of resources for ArcSight Administration here.

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 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.

- The ArcSight ClusterView is for Detect with distributed correlation. This resource group contains all the resources required to monitor the health of Detect 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.

  On the Console, the ClusterView package is located at `/All Packages/ArcSight Foundation/ArcSight ClusterView`.
- 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 the ArcSight Threat Acceleration Program (ATAP) connector as a threat intelligence data feed. The threat intelligence data feed from ATAP is directly imported to Detect 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.

  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.

  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.

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 installation.

Caution: The resources in the ArcSight Administration, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; OpenText 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 Detect, see the ArcSight Detect documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Release Notes, are available on the Detect documentation page.

For detailed information on the ArcSight Detect resources, see the ArcSight Detect Standard Content Resources document, which is available on the Detect 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.

For detailed information about installing Detect, 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 Detect 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`	Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category. 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 *Protected.*
`/System Asset Categories/ Criticality/High`	Categorize all assets that are considered *critical* 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. 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.
`/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 Detect 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, 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 16.

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 36

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 16.

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 36.

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.

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

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

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

To enable rules to send notifications, first configure notification destinations (see "Configuring Notification Destinations" below), then enable the notification 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 rule:ArcSight Administration/Detect/System Health/Resources/Domains/**Out of Domain Fields**.

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/Detect/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
Excessive Rule Recursion	ArcSight Administration/Detect/System Health/Resources/Rules/
Rule Matching Too Many Events	ArcSight Administration/Detect/System Health/Resources/Rules/

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 36 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/Detect 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	
Detect Overview	Provides administration content for monitoring the system.
Detect	
Detect Licensing	Provides information about licensing compliance.
Detect User Sessions	Provides information about user access to the system.
Detect - Configuration Changes	
Detect Resource Configuration Changes	Provides information about changes to the various resources, such as rules and so on.
Detect - System Health	
Detect Events	Provides statistics on the flow of events through the system.
Detect Resource Monitoring	Provides processing statistics for various resources, such as rules, and so on.
Detect Reporting Resource Monitoring	Provides information about performance statistics for query viewers.

Detect Overview

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

Using the Detect Overview Use Case

The **Detect 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 **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 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.

Detect Licensing

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

Using the Detect Licensing Use Case

The **Detect Licensing** use case is located in `/All Use Cases/ArcSight Administration/Detect` 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.

Detect User Sessions

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

Using the Detect User Sessions Use Case

The **Detect User Sessions** use case is located in `/All Use Cases/ArcSight Administration/Detect` 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 Detect (user login and logout activity, including login session and notification information). 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.

- **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 Detect 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 Detect rules are also provided.

Detect Resource Configuration Changes

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

Using the Detect Resource Configuration Changes Use Case

The **Detect Resource Configuration Changes** use case is located in `/All Use Cases/ArcSight Administration/Detect/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 that provide information about recently deleted, created, or updated Detect resources. The Library section of the use case lists supporting resources that help compile information in the dashboard.

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 Detect resource changes by type within the last hour in a pie chart. Detailed information about logs associated with these changes is also provided.

Detect Events

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

Using the Detect Events Use Case

The **Detect Events** use case is located in `/All Use Cases/ArcSight Administration/Detect/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 Detect and non-ArcSight Detect events (including event throughput), active channels that show system monitoring events generated by the local ArcSight Detect system and all events generated by ArcSight. The Library section of the use case lists supporting resources that help compile information in the dashboards and active channels.

Viewing the Dashboards

The **Detect 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 Overview** displays an overview of non-ArcSightDetect events focusing on event counts, events by vendor and product, and by device IP address.
- **Event Throughput** displays event throughput information.
- **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 **Detect 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 ArcSightDetect 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.

Detect Resource Monitoring

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

Configuring the Detect 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 Detect Resource Monitoring Use Case

The **Detect Resource Monitoring** use case is located in `/All Use Cases/ArcSight Administration/Detect/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, queries, and data monitors.

The Library section of the use case lists supporting resources that help compile information in the dashboards.

Viewing the Dashboards

The **Detect Resource Monitoring** use case provides two dashboards. The Rules Status dashboard displays information about the rules engine with detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, and error logs. The Data Monitor Status dashboard displays status about data monitors with detailed information about event count, processing time, DCache Sync Count, and DCache Sync Time.

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

Detect Reporting Resource Monitoring

The Detect Reporting Resource Monitoring use case provides performance statistics for query viewers. No configuration is required for this use case.

Using Detect Reporting Resource Monitoring

The **Detect Reporting Resource Monitoring** use case is located in `/All Use Cases/ArcSight Administration/Detect/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, query viewers, and active channels to help you monitor, investigate and inform on performance statistics for query viewers. The Library section of the use case lists supporting resources that help compile information in the dashboards, query viewers, and active channels.

Viewing the Dashboards

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

Query Viewer Details shows query details for query viewers.

Viewing the Active Channels

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

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

Viewing the Query Viewers

The Detect Reporting Resource Monitoring use case provides three query viewers. To view a query viewer, click the link for the query view in the use case. The query view opens in the Viewer Panel. The query viewers are described below.

Last 10 Query Viewer Queries: Retrieves the last ten query viewer query duration.

Query Viewer Failures During Last 24 hr: Retrieves failed query viewers in the last 24 hours.

Top 10 Longest Query Viewer Queries During Last 24 hr: Retrieves query information for the top 10 longest queries in the last 24 hours.

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.

Use Case	Purpose
Security Threat Monitoring	
"Security Threat Monitoring" on the next page	This use case contains the default security threat monitoring content.
Threat Intelligence Platform	
"Threat Intelligence Platform" on page 31	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.

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 etc. 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 Detect.

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 Detect Default Content on the ArcSight Marketplace and 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 Detect 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. The wizard takes you to the Enable the Following Rules 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.

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
• Application Monitoring

Child Use Cases
Entity Monitoring
• Account Activity • Brute Force Attacks • Unsuccessful User Logins
Host Monitoring
• Host Monitoring
Malware Monitoring
• Malware Monitoring
Network Monitoring
• Attacks and Suspicious Activity Overview • Network Monitoring
Perimeter Monitoring
• Perimeter Monitoring
Vulnerability Monitoring
• 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 Detect 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.
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 Enable or Disable rules screen. Choose which rules to enable or disable.
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 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 Detect 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 Detect 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.

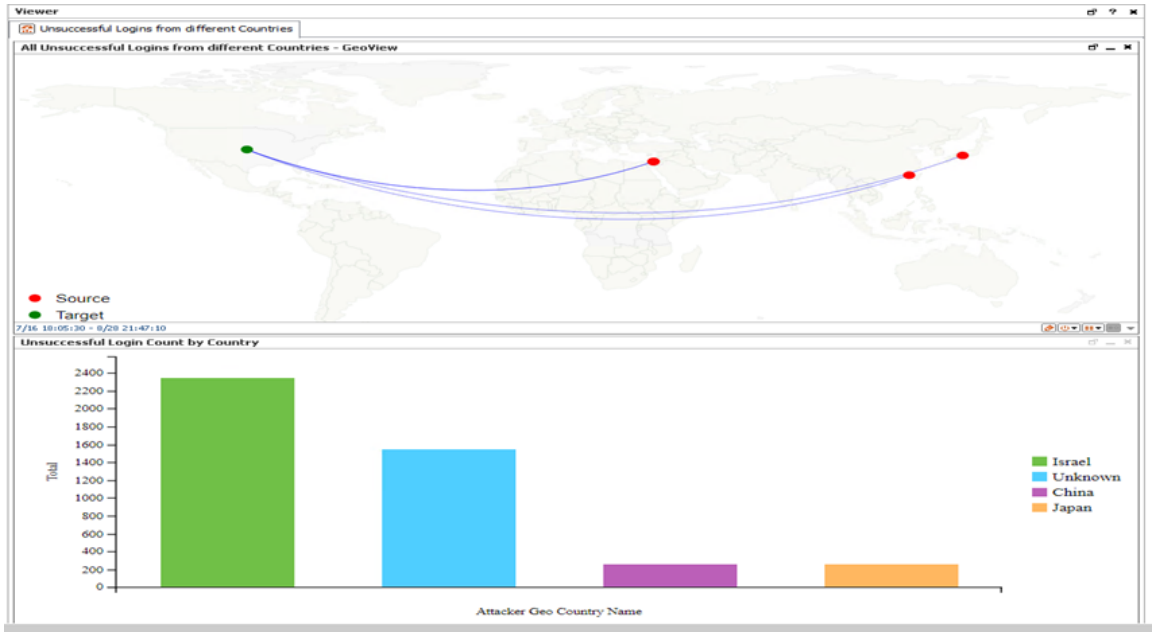
For your reference, an example to use the **Unsuccessful User Login** child use case is given below.

The **Unsuccessful User Login** use case is present at the following location in the Detect 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 ArcSight Threat Acceleration Program (ATAP) connector as a threat intelligence data feed. The threat intelligence data feed from ATAP is directly imported to Detect 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 Detect.

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 Detect 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 Detect 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
```

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
"Priority Formula Resources" on the next page	Includes resources that directly or indirectly affect the Priority Formula.
"System Resources" on page 39	Includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

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 Detect 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 12.

  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 Detect 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 `False`, 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 `False`, 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 for Detect.

Using the System Resources

The System Resources group consists of several active channels that show events received by ArcSight Detect over different periods of time and several integration commands that you can use in ArcSight Detect 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.

Integration Commands

ArcSight Detect 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

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

Active Channels

Name	Description	Location
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

Active Lists

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

Name	Description	Location
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
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
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

Dashboards

Name	Description	Location
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
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
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
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
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
Query Viewer Details	Displays query details for query viewers.	/All Dashboards/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewer Details
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
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

Data Monitors

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
Sortable Rule Stats (only applies to compact mode)	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. 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.	/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

Name	Description	Location
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
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

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

Name	Description	Location
getHourOfDay	Returns hour of manager receipt time.	/All Fields/ArcSight Administration/Detect/Distributed Correlation Monitoring/getHourOfDay
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

Filters

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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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
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.	/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
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.

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
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)
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.	/All Queries/ArcSight Administration/Detect/System Health/Resources/Reporting/Query Viewers/Query Viewer Queries
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

Query Viewers

Name	Description	Location
Hourly EPS Received in Correlator	Displays hourly EPS reveived 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

Name	Description	Location
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

Rules

Rules have individual tables organized by sub folder.

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
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

Name	Description	Location
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
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
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

Session Lists

Name	Description	Location
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
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.	/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 query viewers.	/All Use Cases/ArcSight Administration/Detect/System Health/Detect Reporting Resource Monitoring
Detect Resource Monitoring	Provides processing statistics for various Detect resources.	/All Use Cases/ArcSight Administration/Detect/System Health/Detect Resource 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

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
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
Indicator Types	This list syncs with Suspicious Indicator Types, which is maintained by two lightweight rules.	/All Active Lists/ArcSight Foundation/Common/Indicator Types
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
Interzone Communications to Restricted Services	Contains restricted services.	/All Active Lists/ArcSight Foundation/Common/Interzone Communications to Restricted Services
Suspicious Indicator Types	Contains indicator types which can trigger certain rules.	/All Active Lists/ArcSight Foundation/Common/Suspicious Indicator Types
Suspicious Countries	Contains suspicious countries, for example itar prohibited countries.	/All Active Lists/ArcSight Foundation/Common/Suspicious Countries
Cleartext Protocols	Contains Cleartext Protocols.	/All Active Lists/ArcSight Foundation/Common/Cleartext Protocols
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
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
Ransomware Notes	Contains known ransomware instruction filenames.	/All Active Lists/ArcSight Foundation/Common/Ransomware Notes
Threat Level Mapping	Maps the threat level to the severity and priority.	/All Active Lists/ArcSight Foundation/Common/Threat Level Mapping
MITRE ATT&CK List	Contains Mitre Att&ck information.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/MITRE ATT&CK List
Category for Exploit	Stores categories for exploit.	/All Active Lists/ArcSight Foundation/Common/Category for Exploit
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

Name	Description	Locations
Uncommonly Used Ports	Contains the list of uncommonly used ports.	/All Active Lists/ArcSight Foundation/Common/Uncommonly Used Ports
Commonly Used Ports	Contains the list of uncommonly used ports.	/All Active Lists/ArcSight Foundation/Common/Commonly 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

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
Suspicious Activities Tracking	Tracks suspicious activities.	/All Active Lists/ArcSight Foundation/Common/Suspicious Activities Tracking

Name	Description	Location
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
MITRE Attackers and Targets Relations	Displays the relationship between attacker and target machines using MITRE IDs.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/MITRE Attackers and Targets Relations

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
dc_tgtAddress (tgtAddressByDirection)	Returns the destination addresses for outbound traffic and the source addresses for inbound traffic.	/All Fields/ArcSight Foundation/Common/Orginator by Traffic Direction/dc_tgtAddress
dc_tgtAddressZone (tgtZoneByDirection)	Returns the destination zones for in bound traffic and the source zones for outbound traffic.	/All Fields/ArcSight Foundation/Common/Orginator by Traffic Direction/atkZoneByDirection/dc_ tgtAddressZone
dc_getOrginator (getOrginator)	Returns the string destinations for outbound traffic and the string sources for inbound traffic.	/All Fields/ArcSight Foundation/Common/Orginator by Traffic Direction/dc_getOrginator
dc_atkAddress (atkAddressByDirection)	Returns the destination addresses for outbound traffic and the source addresses for inbound traffic.	/All Fields/ArcSight Foundation/Common/Orginator 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/Orginator 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
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
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
Mitre Details Summary	Selects MITRE details summary.	/All Queries/ArcSight Foundation/MITRE ATT&CK/Mitre Details Summary

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

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.

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.

Use Case	Name	Description
	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.
	User Accounts Added to Group	Stores the information about the user accounts added to groups within the 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.

Use Case	Name	Description
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.

Use Case	Name	Description
	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.
	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.

Use Case	Name	Description
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.
	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.
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	DNS Query Codes	Detects DNS query codes.
	Windows File Inclusions	Detects the most common form of file inclusions to a Windows 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.
	All DNS Events	Detects all the Microsoft and AWS Route53 DNS events.
	DNS Response Codes	Detect DNS response codes.
	Cross Site Scripting from Other Devices	Detects cross-site-scripting attacks from other device vendors.
	AWS Route53 Location DNS Queries	Detects the Route 53 edge location that responded to the query.

Use Case	Name	Description
	Format String Attack Attempts from Other Devices	Detects the format strings attacks captured from IDS, Antivirus and other application devices.
	DNS SubDomains	Detects DNS subdomains requested.
	Directory Traversal Attempts from Other Devices	Detects the Directory Traversal attacks captured from IDS, Antivirus and other application devices.
	Code Injections from Other Devices	Detects the code injection attacks captured from IDS, Antivirus and other application devices.
	DNS NXDOMAIN Events	Detects NXDOMAIN events from DNS servers.
	Linux File Inclusions	Detects the most common form of file inclusions to a Linux server during a code injection attack.
	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.
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.

Use Case	Name	Description
	Brute Force Attack Attempts	Detects correlation events generated by the rules: • Brute Force OS and Application Attempts • Brute Force IDS Detected Attempts
	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.

Use Case	Name	Description
	Attacks and Suspicious Activity	Detects events which indicate compromise, reconnaissance, hostile, or suspicious activity.
	HTRAN Detected	Detects HTRAN signature detected events.
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 wmiprvse.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	Detects sudo command executions. **Linux Note:**To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart the audit service.
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	Detects when azure resource groups are deleted. **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. **False Positives:** Administrator account doing maintenance in the cloud environment.
Azure Runbook Created	Detects when an azure runbook is created in the cloud environment. **Investigation Tip:** Adversaries could create runbooks to execute automate tasks in the azure cloud environment. **False Positives:** Cloud administrator executing administrative tasks in the cloud environment.
Azure Runbook Deleted	Detects when an azure runbook is deleted in the cloud environment. **Investigation Tip:** Adversaries could delete existing azure runbooks to disrupt certain functionalities within the cloud environment. **False Positives:** Administrator account doing maintenance in the cloud environment.
Azure Service Principal Created	Detects when an azure service principal is created. **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. **False Positives:** Administrator account doing maintenance in the cloud environment.
Cloud Account Created	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.
Cloud Firewall Deleted	Detects when any of the firewall features provided by the cloud vendor it is disabled or deleted. **False Positive:** Regular activity performed by cloud administrators.

Name	Description
Cloud Instance Created By Recent User Created	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. **False Positives:** A new administrator account created creating cloud instances.
Cloud Instance Deleted By Recent User Created	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. **False Positives:** A new administrator account deleting cloud instances.
Cloud Instance Snapshot By Recent User Created	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. **False Positives:** A new administrator account creating cloud snapshots.
Cloud Key Vault Deleted	Detects when cloud key storage has been deleted on the cloud environment. **Investigation Tip:** Find out if the user deleting the key vault is authorized to do such activity. **False Positives:** Administrator account doing maintenance in the cloud environment.
Cloud Key Vault Updated	Detects when cloud key storage modified or created on the cloud environment. **Investigation Tip:** Find out if the user updating or creating the key vaults is authorized to do such activity. **False Positives:** Administrator account doing maintenance in the cloud environment.
Cloud Monitoring Disabled	Detects when cloud monitoring has been disabled or deleted from the environment. **False Positives:** Administrator account doing maintenance in the cloud environment.
Cloud Network Monitoring Disabled	Detects when network diagnostic settings have been disabled or deleted on the cloud environment. **Investigation Tip:** Find out if the user account is authorized to carry out any of these activities. **False Positives:** Administrator account doing maintenance in the cloud environment.
Cloud Storage Deleted	Detects when cloud storage was deleted. **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. **False Positives:** Administrator account doing maintenance in the cloud environment.
Email with Malicious Url	Detects emails with malicious Url on Office 365.
Multiple Cloud Firewall Updates	Detects when multiple cloud firewall updates are made by same user account in a short period of time. **False Positives:** Regular Administrator cloud account user performing changes on the environment.

Name	Description
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 AWS Cloud API Activity Detected	Detects suspicious usage of cloud API. This rules is disabled by default.
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.
Command Obfuscation Using PowerShell	Detects command obfuscation using Powershell.
CertUtil used to decode file on host	Detects certutil usage to decode files.
Chained Rule - System Information Discovery	Detects attempts to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. **Linux Note:** In order to capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **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

Name	Description
Changes to Windows Firewall Exception List	Detects modifications to the windows system firewall exception list. **Windows Note:** In order to capture the windows logs,follow the steps below. Enable auditing in the following fields in the group policy editor: Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change. Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields: • Audit Filtering Platform Policy Change • Audit MPSSVC Rule-Level Policy Change • Audit other Policy Change EventsRestart the service mpssvc.
Commands Executed to Create a New Service	Detects abuse to the system via the creation of new services using Command Line tool or PowerShell. **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
COR_PROFILER to Hijack Program Execution Flow	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. **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
Crackmapexec Pass the Hash	Detects Pass the hash (PtH) occurs using crackmapexec.
Credential Dumping via ProcDump and Task Manager	Detects when the ProcDump is used to dump the memory space of Lsass.exe and when credential dumping through window task manager is practiced.
Credential Dumping Using LaZagne	Detects searches for common password storage locations such as databases, mail, and WiFi, to obtain user credentials using LaZagne.

Name	Description
Credentials Gathered using Mimikatz Tool	Detects attempts to extract credential material from the Security Account Manager using Mimikatz.
Credentials In Files	Detects searches of local files and remote file shares for unsecured credentials.
Credentials in Group Policy Preferences	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/ **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
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.

Name	Description
DCOM Instance Creation Attempted	Detects DCOM instance creation attempts via PowerShell.
DCOM Objects Enumeration via PowerShell	Detects enumeration ofDCOM objects via PowerShell.
Delete Backups Using WBadmin	Detects the deletion or removal of built-in operating system data and the turn-off of services designed to aid in the recovery of a corrupted system using WBadmin.
Deletion of Active USN Change Journal Using Fsutil	Detects if an active USN change journal is deleted using fsutil.
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.
Disable Windows System Firewall	Detects disabling of the windows system firewall. **Windows Note:** In order to capture the windows logs, follow the below steps. In order to audit any policy changes in windows, enable auditing in the following fields in the group policy editor: Computer Configuration -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Policy Change. Under the Policy Change fields, there are multiple subcategories. Enable Auditing for the following fields: • Audit Filtering Platform Policy Change • Audit MPSSVC Rule-Level Policy Change • Audit other Policy Change Events Restart the service mpssvc.
Disable Windows Recovery Using BCDedit Tool	Detects the deletion or removal of built-in operating system data and the turn off of services designed to aid in the recovery of a corrupted system to prevent recovery using BCDedit.
Disabled tty_ tickets for Sudo Caching	Detects disabling of tty_tickets for sudo caching. **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.
Event Log Deleted Using Wevtutil Tool	Detects the clearing of Windows Event Logs to hide an intrusion using wevtutil.

Name	Description
DNS-Tunnel Creation Attempted via DNScat	Detects when DNScat is downloaded and DNS Tunnel Creation is Attempted.
External Device With autorun.inf Detected	Detects external drives plugged having autorun.inf
File Copied On Shared Folder	Detects files copied on a shared folder. In order to get these events, you must enable folder auditing in Windows.
File Downloaded On Host	Detects files downloaded using a web browser on the host.
File Encrypted Using Encryptor Tool	Detects attempts to encrypt data on target systems using encryptor.exe.
File or Folder deleted by PowerShell	Detects possible file or folder deletion by PowerShell.
File or Folder Deleted Using cmd.exe	Detects Windows deletion of files and folders using cmd.exe / c.
File or Folder Deletion on Linux	Detects attempts to delete files and folders on the Linux system. To capture this use case, the following steps are needed to be done: 1. Install Snoopy Logging (open source) on the Linux machine that is being monitored. 2. Install Syslog file connector. 3. Provide the path as /var/log/secure in the Syslog connector
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.

Name	Description
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.
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\.
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.

Name	Description
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.
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.

Name	Description
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	Detects abuse odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names. **Windows Note:** To capture the Windows logs, please 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
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.
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.

Name	Description
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	Detects data compression collected using PowerShell. **Windows Note:** To capture the Windows logs, please 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
Possible Change of Default File Association	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. **Windows Note:** To capture the Windows logs, please 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
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.
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 Exfiltration to Text Storage Sites	Creates correlation events for possible exfiltration to text storage sites. This rule includes an Active List with the entries of the URLs of Text Storage Sites. Users can add their own URLs to the existing Active List as entries.

Name	Description
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.
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.

Name	Description
Program Install	Detects adversaries establishing persistent and elevate privileges by using and installer to trigger the execution of malicious content.
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	Detects adversaries looking for information about running processes on a system. **Linux Note:** In order to capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.
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.
Service Modified through Registry Using PowerShell	Detects adversaries modifying system services through registry using powershell commands.

Name	Description
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	Detects adversaries might bypass process and signature-based defenses by proxying execution of malicious content with signed binaries. **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"
Spearphishing via Whatsapp	Detects spearphishing messages via third-party services in an attempt to gain access to systems. Spearphishing via service is a specific variant of spearphishing.
Specific Processes Killed Using PowerShell Command	Detects specific stopped or disabled processes on a system.
Sudoers File Modified	Detects adversaries trying to modify the sudoers file in the Linux system. **Linux Note:** To capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # 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. Restart the audit service.
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.

Name	Description
Suspicious Activity after Modify Service	Detects suspicious activities after modifying a service.
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.

Name	Description
Suspicious File Discovery Activity On Host	Detects multiple file extensions accessed on the same machine in short period of time.
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	Detects windows processes executed from suspicious locations. 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.
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.

Name	Description
Suspicious Uncommonly Used Port Events by Script	Detects commonly used port event launched by a script.
System Information Discovery	Detects adversaries attempting to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. **Linux Note:** To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **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"
System Process Discovery	Detects adversaries looking for information about running processes on a system. **Linux Note:** In order to capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.
SystemRestore Task Disabled Using Schtasks	Detects abuse to task scheduling functionality to facilitate initial orrecurring execution of malicious code using Schtasks.
Track Job Scheduling Change	Detects changes of the file /etc/crontab.
Track Modified Service	Tracks modified services.

Name	Description
Track New Service	Tracks new services.
Track Scheduled Task	Tracks schedule tasks and writes them down on Suspicious Activities Tacking Active List.
UAC ByPass Registry Key Changed	Detects changes to an entry relevant to UAC Bypass.
Unlimited Sudo Cache Timeout Set	Detects when an adversary sets unlimited sudo cache timout. 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.
Unusual Microsoft Office Network Connections	Detects unusual traffic generated by Microsoft Office applications.
Unusual Windows Process Relationship	Detects unusual parent - child windows system process relationships.
Virtual Machine Environment Discovery Using Registry	Detects when an adversary interacts with the Windows Registry to gather information about the system, configuration, and installed software. **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
Windows Admin Share Accessed	Detects when a windows admin shared has been accessed.
Windows File Deleted Using Sdelete	Detects Sdelete command executions.
Windows Firewall Rule Changed by netsh command	Detects windows firewall rule changed by netsh command.
Windows Firewall Rule Discovery	Detects queries made on registry that keeps Windows Firewall Rules.

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	Detects adversaries trying to abuse Windows Management Instrumentation (WMI) to achieve execution. **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

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: • 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 IFEO (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	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 . **Linux Note:** To capture the Linux logs, include the below rules in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the below rule to the file: -w /etc/login.defs -p wa -k password_policy_modified -w /etc/pam.d/system-auth -p wa -k password_policy_modified 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. Restart audit service.
Multiple Queries to Registry for Discovery	Detects adversaries interacting with the Windows Registry to gather information about the system, configuration, and installed software. **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"
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	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. **Linux Note:** To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the rule below to the file: -w /etc/login.defs -p rx -k password_policy_discovered -w /etc/pam.d/system-auth -p rx -k password_policy_discovered 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. Restart audit service. **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 https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder
Possible Data Exfiltration	Detects suspicious amount of data transferred to any host outside the protect network.
Possible Horizontal Scan Detected	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. Note : A horizontal scan is described as scan against a group of IPs for a single port.
Possible Vertical Scan Detected	Detects adversaries attempting to scan multiple destination ports. By default, the aggregation is set to 20 hits in 1 minute. Note: A vertical scan is described as a single IP being scanned for multiple ports.
Privilege Escalation Attempt Detected	Detects privileged exploit attacks through various ways gathering information from IDS.

Name	Description
Reconnaissance Activity Detected	Detects reconnaissance activity.
Remote System Discovery	Detects adversaries looking for details about other systems by IP address, hostname, or other logical identifiers on a network. **Linux Note:** To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve # For monitoring particular file location, we have to add the rule below to the file: -w /etc/hosts -p rwa -k hosts_file_access 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. Restart audit service. **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. https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/apply-a-basic-audit-policy-on-a-file-or-folder
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	Detects adversaries looking for details about the network configuration and settings of systems they access. **Linux Note:** To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service.
System Network Connections Discovery	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. **Linux Note:** To capture the Linux logs, include the rules below in the audit.rules file in your Linux Machine. Path: /etc/audit/audit.rules Include the below rules based on the linux architecture: -a exit,always -F arch=b64 -F euid=0 -S execve -a exit,always -F arch=b32 -F euid=0 -S execve Restart audit service. **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 **PowerShell Note:** To capture the PowerShell logs, make necessary modifications as per the below connector guide link. https://community.microfocus.com/dcvta86296/attachments/dcvta86296/connector-documentation/1290/2/MSPowershellWinEvtLog_N.pdf
Vulnerability Scanning	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 insidera trying to do a vulnerability scan to target a victim machine.

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. • 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. • 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.

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
Very High Confidence Alerts	Monitors very high confidence alerts from suspicious sources and suspicious hashes.	/All Active Channels/ArcSight Foundation/Threat Intelligence Platform/Very High Confidence Alerts

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

Name	Description	Location
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 ATAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Addresses List
Suspicious Domain List	Contains suspicious domains collected from ATAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain List
Suspicious Email List	Contains suspicious emails collected from ATAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email List
Suspicious Hash List	Contains suspicious hash collected from ATAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash List

Name	Description	Location
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 ATAP.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Suspicious URL List
Track ATAP Connector	Stores information when the ATAP SmartConnector receives or processes data. 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.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Track ATAP Connector
Track ATAP Connector Type	Stores the ATAP connector name and type.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/Track ATAP Connector Type
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
Additional Suspicious Hash*	Define suspicious hash.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/Additional Suspicious Hash

Name	Description	Location
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
ATAP Health Status	This dashboard shows the latest status of ATAP 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/ATAP Health Status
Data Feed Overview	Displays data feed overview by creatororg, confidence, attribute type, and most active threat actors.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview

Name	Description	Location
TI Confidence Comparison-Open Source vs ArcSight-curated	Allows you to monitor the confidence comparison between ArcSight and open-source TI feeds.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Compariso-Open Source vs ArcSight-curated
TI Confidence Details	Displays a confidence reputation data overview.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/TI Confidence Details
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
Top Malware and CVE	Allows you to monitor datafeeds sorted by malware, AV signature, 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

Data Monitor

Name	Description	Location
ATAP Connector Status	Shows the latest status of ATAP 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/ATAP Connector Status

Field Set

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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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

Name	Description	Location
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
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
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 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
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) is 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 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
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

Name	Description	Location
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
Source in Suspicious Email List APT Malware Related	Identifies the source username (email address) is 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) is 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
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
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/Threat Level High
Threat Level Medium	Returns eturns all events with threat level medium: APT Malware Related.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/Filter By Threat Level/Threat Level Medium

Name	Description	Location
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 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 ATAP Connector	Selects updated events from ATAP Connector.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Update events from ATAP 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
Update events from ATAP Connector	Selects updated events from ATAP Connector.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Update events from ATAP Connector

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
ArcSight-curated Threat Intelligence Feed	Selects data feed counts grouped by confidence in which the creator organization is ArcSight.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/ArcSight-curated Threat Intelligence Feed
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

Name	Description	Location
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
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 Indicator Type	Selects data feed overview by malware type.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Indicator Type/Data Feed Overview by Indicator Type
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
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
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
High Confidence ArcSight-curated Threat Intelligence Feed	Selects data feed counts grouped by confidence in which the creator organization is ArcSight.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Confidence/High Confidence ArcSight-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

Name	Description	Location
Most Active Threat Actors	Selects most active actors.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/Data Feed Overview/Most Active Threat Actors
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
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
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
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
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

Name	Description	Location
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
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 ArcSight-curated TI Feed	Displays high confidence ArcSight-curated TI feed.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/Actionable IoC's from ArcSight-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
ArcSight-curated Threat Intelligence Feed	Displays data feed overview grouped by confidence in which the creator organization is ArcSight.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Confidence/ArcSight-curated Threat Intelligence 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

Name	Description	Location
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
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
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
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
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

Name	Description	Location
Malware and AV Details	Displays malware and AV details.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/Malware and AV/Malware and AV Details
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
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
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

Name	Description	Location
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
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
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
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

Name	Description	Location
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, 0day 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
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

Name	Description	Location
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
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

Name	Description	Location
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
Command and Control Multiband Communication	Detects plit 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. This rule is dependent on the rule /All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/Inbound Suspicious Traffic.	/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
Outbound Communication to a Malvertising Publishing Domain	Detects malvertising communication to publishing domains.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing /Outbound Communication to a Malvertising Publishing Domain
Outbound Communication to Malvertising Publishing Address	Detects malvertising communication to publishing addresses.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/Outbound Communication to Malvertising Publishing Address

ATAP Connector Health

Name	Description	Location
Error in ATAP Connector Service Message	Detects ATAP Connector errors receiving or processing a malicious list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Error in ATAP Connector Service Message
No Update from ATAP Connector	Detects if any entries expire from the Track ATAP 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/ATAP Connector Health/No Update from ATAP Connector
Track ATAP Connector Service Message	Tracks ATAP Connector service message events and adds them to an active list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Track ATAP Connector Service Message
Track ATAP Connector Update Count	Tracks ATAP connector update counts and sends them to an active list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Track ATAP Connector Update Count
Track ATAP Connector Type	Detects events of connector type.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/ATAP Connector Health/Track ATAP Connector Type

High Confidence Alerts

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

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: Not Released

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 (Detect 8.1.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!