Micro Focus Security ArcSight ESM RepSM Plus

Software Version: 1.8

Solutions Guide

MICRO FOCUS®

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

Support

Contact Information

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

Contents

Chapter 1: Overview and Architecture

This chapter discusses the following topics:

How Reputation Security Monitor Plus Works

The Micro Focus Reputation Security Monitor Plus (RepSM Plus) solution uses internet threat intelligence to detect malware infection, zero day attacks, and dangerous browsing on your network. RepSM Plus consists of the following components:

- The Micro Focus RepSM Plus service provides reputation data from the comprehensive database of malicious IP addresses and domain names. RepSM Plus uses IPv4 and Domain Name System (DNS) security intelligence feeds from multiple sources to provide a broad set of reputation data.
- The Micro Focus Model Import Connector for RepSM Plus imports the reputation data at regular intervals from the RepSM Plus service to ArcSight ESM or ESM Express.
- The Micro Focus RepSM Plus content running on ArcSight ESM or ESM Express, correlates the reputation data and security events to detect and remediate security incidents and issues that would otherwise be undetectable. RepSM Plus content is organized into several use cases, which address specific objectives.

The following figure shows how RepSM Plus components work together.
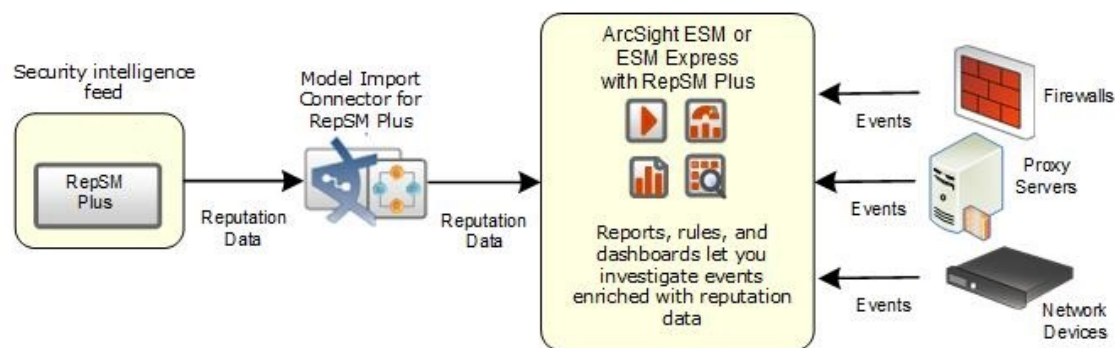
What RepSM Plus Can Do for You

By analyzing communications with known disreputable internet hosts, RepSM Plus can help you achieve the following objectives:

- "Protect from Advanced Persistent Threats (APTs)" below
- "Detect and Analyze Zero Day Attacks" below
- "Provide Insight into Malicious Communications" below
- "Ensure the Reputation of Your Organization's Assets" on the next page
- "Optimize the Security Operations Center" on the next page

Protect from Advanced Persistent Threats (APTs)

APTs are sophisticated cyber attacks in which an adversarial group targets previously identified computers and installs malware on those computers. The malware then establishes communications with an external command and control center, and extracts information from your network. APTs typically operate undetected for an extended period of time, however, RepSM Plus enables you to:

- Detect APTs early by correlating events regarding communication from internal computers to external command and control centers.
- Analyze the past activity of infected computers for forensic investigation by using the ArcSight Logger integration commands.

The Internal Infected Assets use case provides resources to perform these activities.

Detect and Analyze Zero Day Attacks

Zero day attacks exploit newly found software vulnerabilities before vendors have the opportunity to correct the vulnerability. By detecting successful communications to internal assets from disreputable sources, RepSM Plus provides early detection of attacks that would not be detected by standard, signature based security controls.

The Zero Day Attacks use case provides a dashboard of this inbound traffic.

Provide Insight into Malicious Communications

RepSM Plus detects malicious communication based on reputation data and then uses correlation rules to identify a scenario that further explains the nature of the communication. For more information, see "RepSM Plus Scenarios" on page 11.

The General Scenarios use case provides a dashboard of inbound and outbound malicious communication during the last seven days.

Ensure the Reputation of Your Organization's Assets

RepSM Plus can provide an early warning that your organization's assets have been included in the reputation database, indicating a potential security breach. Conversely, assets might be falsely included in the database, but still require investigation to avoid negative operational effects, such as e-mail from your organization being marked as spam.

The Internal Assets Found in Reputation Data use case focuses on assets that have been listed in the reputation database and require attention.

Optimize the Security Operations Center

RepSM Plus enables security analysts to analyze events within the context of global threat intelligence to avoid false positives and focus on key events. By correlating events with reputation data, RepSM Plus can depict risk more accurately in reports and dashboards.

The Event Enrichment with Reputation Data use case provides global variables that you can use to add reputation intelligence to non-RepSM Plus resources.

Reputation Data

RepSM Plus stores the reputation data from the RepSM Plus service in active lists; one list for IP addresses and another list for domain names. Those active lists are collectively referred to as the *reputation database*. Each IP address or domain name in the *reputation database* has a *reputation score* and *exploit type*, as described in the following sections. The RepSM Plus use cases detect various kinds of malicious activity based on the reputation scores and exploit types.

You can also add or exclude IP addresses and domain names by customizing the active lists described in "Including and Excluding Entries from Reputation Data" on page 20.

Reputation Scores

The reputation score is a number from 0 to 100 that indicates the potential security risk of the IP address, host name, or domain name, based on current threat intelligence from the reputation database. The higher the score, the greater the potential for risk. Scores

below 40 represent undesirable but not malicious activity. Scores below 20 are unlikely to pose any threat.

> **Note:** Entities with a score of 0 pose no threat at all, but are maintained in the reputation database because they are considered candidates for malicious activity. By default, the RepSM Plus use cases ignore entities that have a score of 0.

Exploit Types

The exploit type indicates the threat attributed to the malicious host, as described below:

Type	Description
Ad Fraud	Sites that are being used to commit fraudulent online display advertising transactions using different ad impression boosting techniques including but not limited to the following, ads stacking, iframe stuffing, and hidden ads. Sites that have high non-human web traffic and with rapid, large and unexplained changes in traffic.
Blended Threat	The malicious host is classified as having multiple exploit types.
Botnet	Bots are compromised machines running software that is used by hackers to send spam, phishing attacks, and denial of service attacks.
Command and Control Centers	Internet servers used to send commands to infected machines called "bots."
Compromised & Links To Malware	Web pages that appear to be legitimate, but house malicious code or link to malicious websites hosting malware. These sites have been compromised by someone other than the site owner. If Firefox blocks a site as malicious, use this category. Examples are defaced, hacked by, and so on.
Malware Call-Home	When viruses and spyware report information back to a particular URL or check a URL for updates, this is considered a malware call-home address.
Malware Distribution Point	Web pages that host viruses, exploits, and other malware are considered Malware Distribution Points. Web Analysts may use this category if their anti-virus program triggers on a particular website. Other categories should also be added if applicable.
Malware	The malicious host is one of the following: • A web server that distributes malware to users who browse sites located on the server. • A command and control center for computers infected with malware.
Miscellaneous	The host is considered malicious, but there is insufficient information to classify it as another, more specific exploit type.
Misuse and Abuse	The malicious host scans the internet for vulnerable systems, or serves adult content.
P2P	The malicious host is part of a peer-to-peer (P2P) network, such as eMule or BitTorrent. The malicious host might be the central node for the network or a member of the network.

Type	Description
Phishing	The malicious host sends phishing emails, or the malicious host's URL appears in the text of phishing emails.
Phishing/Fraud	Web pages that impersonate other web pages usually with the intent of stealing passwords, credit card numbers, or other information. Also includes web pages that are part of scams such as a "419" scam where a person is convinced to hand over money with the expectation of a big payback that never comes. Examples con, hoax, scam, and so on.
Spam	The malicious host sends spam emails.
Spam URLs	URLs that frequently occur in spam messages.
Spyware	The malicious host distributes spyware or other suspicious software.
Spyware & Questionable Software	Software that reports information back to a central server such as spyware or keystroke loggers. Also includes software that may have legitimate purposes, but some people may object to having on their system.
Web Application Attacker	The malicious host initiates application layer attacks, such as SQL injection and Cross Site Scripting, against web servers.
Worm	The malicious host is infected by a worm.

RepSM Plus Scenarios

RepSM Plus detects malicious communication based on reputation data. It then uses correlation rules to identify a more granular scenario to explain the nature of the communication. Scenarios can help you determine what action to take. Because a scenario is based on rules, you can create custom scenarios for your organization. The following table describes the scenarios that are provided with RepSM Plus. The General Scenarios use case provides a dashboard of malicious communication events over the last seven days, broken down by scenario.

For information about creating custom scenarios, see .

Scenario	Direction of Communication	Outcome of Communication	Malicious Host Exploit Type	Asset or Activity Detected
Dangerous Browsing	Outbound to malicious host	Success and failure	Phishing, Malware, Compromised & Links to Malware, Malware Call-Home, Malware Distribution Point, Phishing/Fraud	Assets not categorized as Public-Facing and events that have a URL request and the port is 80 or 443
Internal Infected Assets	Outbound to malicious host	Success and failure	Botnet, Command and Control Centers, Compromised & Links to Malware, Spyware & Questionable Software	Assets not categorized as Public-Facing Note: If you classify assets as Public Facing, the use case produces better results and fewer false positives. If you do not classify assets in this category, the use case applies to all assets.
			All Exploit Types	Assets categorized as Public-Facing
Port Scan	Inbound from malicious host	Success and failure	Blended Threat, Botnet, Miscellaneous, Misuse and Abuse, Spyware, Web Application Attacker, Worm	Communication from the same malicious host to the same internal asset, occurring, by default, eight times within two minutes, using different ports
Potential Spear Phishing	Inbound from malicious host	Success and failure	Phishing, Spam, Spam URLs, Phishing/Fraud	

Scenario	Direction of Communication	Outcome of Communication	Malicious Host Exploit Type	Asset or Activity Detected
Peer-to-Peer	Inbound from malicious host	Success and failure	P2P	
Potential Intrusion	Inbound from malicious host	Success and failure	Blended Threat, Botnet, Miscellaneous, Misuse and Abuse, Spyware, Web Application Attacker, Worm	Communication from the same malicious host to the same internal asset, occurring, by default, eight times within two minutes, using the same port
Zero Day Attacks	Inbound from malicious host	Success	Botnet, Command and Control Centers, Miscellaneous, Misuse and Abuse, Spyware & Questionable Software, Web Application Attacker, Worm	Assets categorized as Internal Non Public-Facing

If you classify assets as Public Facing, the use case produces better results and fewer false positives. If you do not classify assets in this category, the use case applies to all assets.

Integration Commands

RepSM Plus provides the following integration commands, which can be invoked from the ArcSight Console:

- The ArcSight Logger commands query historical activity of infected assets. See the topic on "Logger Search Commands" in the *ArcSight Console Guide*.
- The Google web search command finds information about a malicious host. See .

Pattern Discovery

RepSM Plus provides Pattern Discovery profiles to help you detect subtle, specialized, or long-term patterns in the flow of events. These profiles enable you to investigate the following:

- Behavior of Internal Infected Assets
- Complex Attacks Investigation
- Potential Intrusion Investigation
- Zero Day Investigation

For more information, see "Use Pattern Discovery in Your Investigation" on page 31.

Supported Devices

Any event that identifies a source or destination host (through its host name or IP address) or a request URL that contains similar information, applies to the RepSM Plus use cases. The following device types typically produce those events:

- Firewalls
- Intrusion Prevention Systems (IPS)
- Network equipment, such as routers, switches, and wireless access points
- Network monitors, managers, and traffic analyzers
- Virtual Private Networks (VPNs)
- Web proxy servers

Chapter 2: Installing RepSM Plus

Perform the installation tasks in the following order:

1. Verify your environment.
2. Increase the maximum capacity for active lists.
3. Install the content package (.arb file).
4. Install the Model Import Connector for RepSM. See *RepSM Plus Model Import Connector Configuration Guide* and the *RepSM Plus Model Import Connector Release Notes* for details.
5. Configure RepSM Plus content ("Configuring RepSM Plus Content" on page 19). Minimally, you must deploy the RepSM Plus rules to ensure that the use cases produce results.

Verifying Your Environment

Before you install RepSM Plus, make sure that you are running ArcSight ESM or ESM Express 7.0, with or without patches.

RepSM Plus requires the ArcSight Manager to have a minimum of 16 GB Java heap memory size. ArcSight ESM and ESM Express 7.0 by default are configured for 16 GB, and therefore are set to support RepSM Plus. For other ESM versions, verify that you have the minimum requirement for Java heap memory value.

> **Note:** If the Java heap memory size is not set to 16 GB, the installation fails.

Configuring Active List Capacity (Required)

Before you install the RepSM Plus content on either ArcSight ESM or ESM Express, the active list capacity must be increased to 1,500,000 entries to enable RepSM Plus to monitor that number of reputation data entries.

To increase the active list maximum capacity:

1. Add the following line to the server.properties file located in `<ARCSIGHT_HOME>\config`:

   `activelist.max_capacity=1500000`
2. Restart the ArcSight Manager for the new setting to take effect.

For more information about the `server.properties` file, see the Configuration chapter of the *ArcSight ESM Administrator's Guide*.

If you fail to increase the active list capacity, the installation of the RepSM Plus content package will fail with the following error:

```
Install Failed: ActiveList capacity cannot be greater than nnnnnn
```

`nnnnnn` will vary depending on whether you are installing RepSM Plus on ArcSight ESM or ArcSight Express.

Installing the RepSM Plus Content

Follow the procedure below to install the RepSM Plus content package on ArcSight ESM or ESM Express.

> **Note:** The RepSM Plus content is a self-contained solution that does not rely on any other ArcSight solution. You can install the RepSM Plus content package alongside other solutions on the same ArcSight Manager. Before installing a new solution, Micro Focus recommends that you back up any existing solutions installed on the ArcSight Manager.

To install the RepSM Plus content package:

1. Make sure the maximum capacity for active lists is set to 1,500,000, as described in "Configuring Active List Capacity (Required)" on the previous page.

2. Download the following RepSM Plus content package bundle to the machine where the ArcSight Console is installed:

   `Reputation_Security_Monitor_Plus_1.8.arb`

   > **Note:** Internet Explorer sometimes converts the ARB file to a ZIP file during download. If this occurs, rename the ZIP file back to an ARB file before importing.

3. Log into the ArcSight Console as administrator.

4. In the Navigator panel, click the **Packages** tab.

5. Click the **Import** button (⬇).

6. In the Packages for Installation dialog, make sure that the check box is selected next to the name of the RepSM Plus package you want to install and click **Next**.

   The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the summary report.

7. In the Installing Packages dialog, click **OK**.

8. In the Importing Packages dialog, click **OK**.

9. On the Packages tab of the Navigator panel, expand the `/All Packages/ArcSight Solutions/Reputation Security Monitor Plus 1.8` package to verify that the package installation succeeded and that the content is accessible in the Navigator panel.

   If you do not see the RepSM Plus content, see "Troubleshooting the Installation" below.

If the package installation succeeded, you are now ready to configure RepSM Plus content.

Troubleshooting the Installation

If you attempted to install the RepSM Plus content package before increasing the active list capacity, and the installation failed, the RepSM Plus package might become hidden in the list of packages on the Packages tab. If you attempt to re-import the package, you might see the following message:

```
Packages that Don't Need to be Imported:

/All Packages/ArcSight Solutions/Reputation Security Monitor Plus 1.8
```

To display the originally imported RepSM Plus package, click the **Package** icon on the Packages tab, shown highlighted in the figure below.
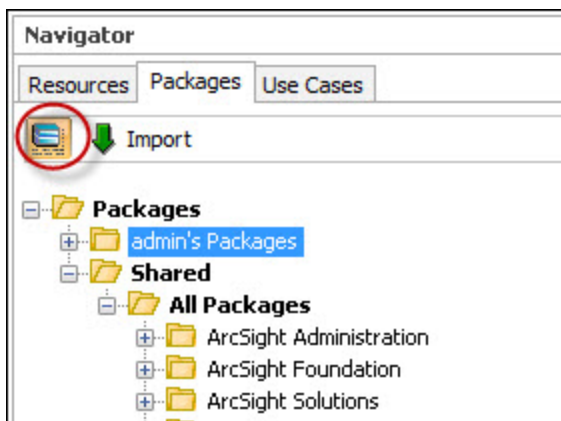
You can then uninstall and reinstall the package.

Installing the Model Import Connector for RepSM Plus

The Model Import Connector for RepSM Plus forwards reputation data from the RepSM Plus service to ArcSight ESM or ESM Express. An active subscription to the RepSM Plus service is required. If you do not have an active RepSM Plus service subscription and would like to purchase one, contact your Micro Focus ArcSight sales representative.

To install and configure the Model Import Connector for RepSM Plus, follow the instructions in the *Model Import Connector for RepSM Plus Configuration Guide*.

Chapter 3: Configuring RepSM Plus Content

Several of the RepSM Plus content resources need to be configured with values specific to your environment. Depending on the features you want to implement and how your network is set up, some configuration is required and some is optional. The list below shows the general configuration tasks for the RepSM Plus resources. Specific configuration tasks for the RepSM Plus use cases are described in "Using RepSM Plus Content" on page 30.

- "Assigning User Permissions" below
- "Including and Excluding Entries from Reputation Data" on the next page
- "Configuring Internal Assets Found in Reputation Data" on page 22
- "Configuring Exploit Types" on page 21
- "Categorizing Assets" on page 22
- "Deploying Rules" on page 24
- "Configuring the Integration Command for Google Search" on page 24
- "Setting Thresholds for the Reputation Score" on page 25
- "Creating Custom Scenarios" on page 26
- "Enabling Trends" on page 27
- "Configuring Cases" on page 28
- "Verifying RepSM Plus Content Configuration" on page 28

Assigning User Permissions

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

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

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

- Active Channels
- Active lists

- Cases

- Dashboards

- Data monitors

- Field Sets

- Filters

- Integration Commands

- Pattern Discovery

- Queries

- Query Viewers

- Reports

- Rules

- Trends

To assign user permissions:

1. Log into the ArcSight Console as administrator.

2. For each of the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type (for example, Active Channels) and navigate to `ArcSight Solutions/Reputation Security Monitor Plus.`

   b. Right-click the Reputation Security Monitor Plus group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.

   c. In the ACL editor of the Inspect/Edit panel, select the user groups for which you want to grant permissions to the RepSM Plus resources and click **OK**.

3. Repeat for each resouce as listed above.

Including and Excluding Entries from Reputation Data

The RepSM Plus active lists retain data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters and rules.

Use the following active lists to define IP addresses and domains that you consider malicious, even if they never appear in the reputation data provided by the RepSM Plus service:

Use the following active lists to define IP addresses and domains that you consider safe, even if they do appear in the reputation data:

- Exceptions - IPs
- Exceptions - Domains

These active lists are used by all of the RepSM Plus use cases and are located in `/ArcSight Solutions/Reputation Security Monitor Plus/User Defined Reputation Data`.

To update any of these active lists, you need to specify either the IP address or domain name.

> **Note:** Domain names must be entirely lowercase.

To update the Additional Malicious IP Addresses and Additional Malicious Domains active lists, you also need to specify a reputation score (1 to 100) and an exploit type. Be sure to specify one of the exploit types described in "Exploit Types" on page 10.

For detailed instructions on adding entries to active lists, see the *ArcSight Console User's Guide*.

Configuring Exploit Types

The following active lists contain default exploit types for the use cases listed below, but you can add or remove exploit types as needed:

Active List	Used by this Use Case
Critical Exploit Types	"Internal Infected Assets" on page 41
Dangerous Browsing Exploit Types	"Dangerous Browsing" on page 32
Zero Day Attack Exploit Types	"Zero Day Attacks" on page 46

For specific configuration information, see the "Configuration" section in the use case sections listed above. For a description of exploit types, see "Exploit Types" on page 10.

For detailed instructions on adding entries to active lists, see the *ArcSight Console User's Guide*.

Using the RepSM Plus Event Filter

RepSM Plus processes events from the devices described in "Supported Devices" on page 14. However, there might be situations in which you want to exclude certain events.

Use the Event Limit filter to control which events are processed by RepSM Plus. This filter is included, either directly or indirectly, in the conditions of all the other resources in the RepSM package, such as rules, queries, and filters. The filter is located in:

```
/All Filters/ArcSight Solutions/Reputation Security Monitor
Plus/General/Event Limit
```

The filter has a default condition value of True, so all events are analyzed. Edit the filter and change the condition to exclude the events that do not interest you.

Configuring Internal Assets Found in Reputation Data

The following active lists require configuration to ensure that the Internal Assets Found in Reputation Data use case produces results:

- Internal Domains for Reputation Monitoring
- Internal Network Addresses for Reputation Monitoring
- Internal Assets for Reputation Monitoring

Note: You can run the Internal Assets Found in Reputation Data report to identify assets in your network that are currently included in the reputation data. For assets that are not accessible to the public, consider adding them to the Exceptions active lists.

For detailed instructions on adding entries to active lists, see the *ArcSight Console User's Guide.*

Categorizing Assets

Categorizing assets adds valuable context to the events evaluated by the RepSM Plus use cases. The RepSM Plus content relies on the following asset categories to distinguish between internal, public, and non-public assets:

Asset Category	Description	URI
Protected	This standard asset category classifies internal assets (those that are inside your organization's network). By default, any address contained in the Private Address Space Zones is categorized as Protected.	`All Assets/Site Asset Categories/Address Spaces`
Public-Facing	This RepSM Plus asset category classifies internal assets that are accessible from the internet.	`/All Assets/ArcSight Solutions/Reputation Security Monitor Plus`
Internal Non Public-Facing	This RepSM Plus asset category classifies internal assets that are not accessible from the internet.	`All Assets/ArcSight Solutions/Reputation Security Monitor Plus`

Asset categorization is required to activate some use cases, and optional but recommended for other use cases to ensure better results with fewer false positives. The following table lists the use cases that rely on asset categorization. For more information, see the use case section referenced in the following table.

Use Case	Asset Category	Categorization is:
"Dangerous Browsing" on page 32	Public-Facing	Recommended
"Internal Infected Assets" on page 41	Public-Facing	Recommended
"Zero Day Attacks" on page 46	Internal Non Public-Facing	Required

For more information about how categorization affects the use cases, see "RepSM Plus Scenarios" on page 11.

How to Assign Asset Categories

The RepSM Plus asset categories can be assigned using one of the following methods:

One by One Using the Console

Use this method if you have only a few assets to categorize. An asset can be categorized in more than one RepSM Plus asset category. For more information, see the *ArcSight Console User's Guide*.

ArcSight Asset Import Connector

If you have many assets to categorize, you can use the ArcSight Asset Import Connector. The ArcSight Asset Import Connector is available as part of the SmartConnector download. For instructions about how to use this connector to categorize your assets for RepSM Plus, see the *ArcSight Asset Import SmartConnector Configuration Guide* and the accompanying Release Notes, if any.

Network Model Wizard

The Network Model wizard provides the ability to quickly populate the ArcSight network model by batch loading asset and zone information from Comma Separated Files (CSV) files. The wizard is available from the ArcSight Console menu option Tools > Network Model. For more information about the wizard, see the *ArcSight Console User's Guide*.

Deploying Rules

For the RepSM Plus rules to process events, the rules must be deployed to the Real-time Rules group. For ESM Express, the rules are deployed by default after RepSM Plus is installed. For ArcSight ESM, you must deploy the rules as described below.

To deploy the RepSM Plus rules to the Real-time Rules group:

1. In the Navigator panel Resources tab, go to Rules and navigate to the `All Rules/ArcSight Solutions/Reputation Security Monitor Plus` group.

2. Right-click the `Reputation Security Monitor Plus` group and select **Deploy Real-time Rule(s)**.

After a few seconds, the rules in the group are listed under the `Real-time Rules/Reputation Security Monitor Plus` group.

The rules in this group are linked to the rules in the `All Rules/ArcSight Solutions/Reputation Security Monitor Plus` group.

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

Configuring the Integration Command for Google Search

To configure the Search Selected Item in Google command to use another search engine:

1. In the Navigator panel Resources tab, select **Integration Commands** and select the **Commands** tab.

2. Navigate to

   `/All Integration Commands/ArcSight Solutions/Reputation Security Monitor Plus`

3. Right-click **Search Selected Item in Google** and select **Edit Command**.

4. In the Inspect/Edit panel, click the **URL** text and overtype `www.google.com` with your preferred search engine URL.

5. Click the **Name** text and overtype `Google` in the command name to indicate your preferred search engine.

6. Optional: Update the Description field to document your changes.

7. Click **OK**.

Setting Thresholds for the Reputation Score

Several RepSM Plus use cases provide rules that rely on a reputation score threshold. Only IP addresses and domain names that have a score equal to or greater than the threshold are considered malicious by the use cases.

You can set different thresholds for the domain names and IP addresses. By default, the thresholds are set to 1, so reputation scores from 1 to 100 are considered.

The following table describes the threshold defined in several global variables provided by the use cases.

Reputation Score Threshold Variables

Variable	Use Case
• Dangerous Browsing Reputation Domain Score Threshold • Dangerous Browsing Reputation IP Score Threshold	"Dangerous Browsing" on page 32
• Internal Infected Assets Reputation Domain Score Threshold • Internal Infected Assets Reputation IP Score Threshold	"Internal Infected Assets" on page 41
• Zero Day Attacks Reputation Domain Score Threshold • Zero Day Attacks Reputation IP Score Threshold	"Zero Day Attacks" on page 46

By default, these variables use the same generic variable, `solnGenericHighScoreThreshold`, which defines the score threshold for both IP addresses and domains.

To change the thresholds, you can either set the threshold in the generic variable, which will affect all of the use cases listed in the Reputation Score Threshold Variables table, or you can override the generic variable and specify thresholds in the individual use cases, as described in the following procedures.

To set the threshold in the generic variable:

1. From the Navigator panel Resources tab, select **Field Sets** from the drop-down list, click the **Fields & Global Variables** tab, and then navigate to:

```
/All Fields/ArcSight Solutions/Reputation Security Monitor
Plus/Configuration
```

2. In the Reputation Score Threshold Variables table, double-click
   solnGenericHighScoreThreshold to open it in the Inspect/Edit panel.

3. Click the **Parameters** tab and change one of the Number arguments, as shown:
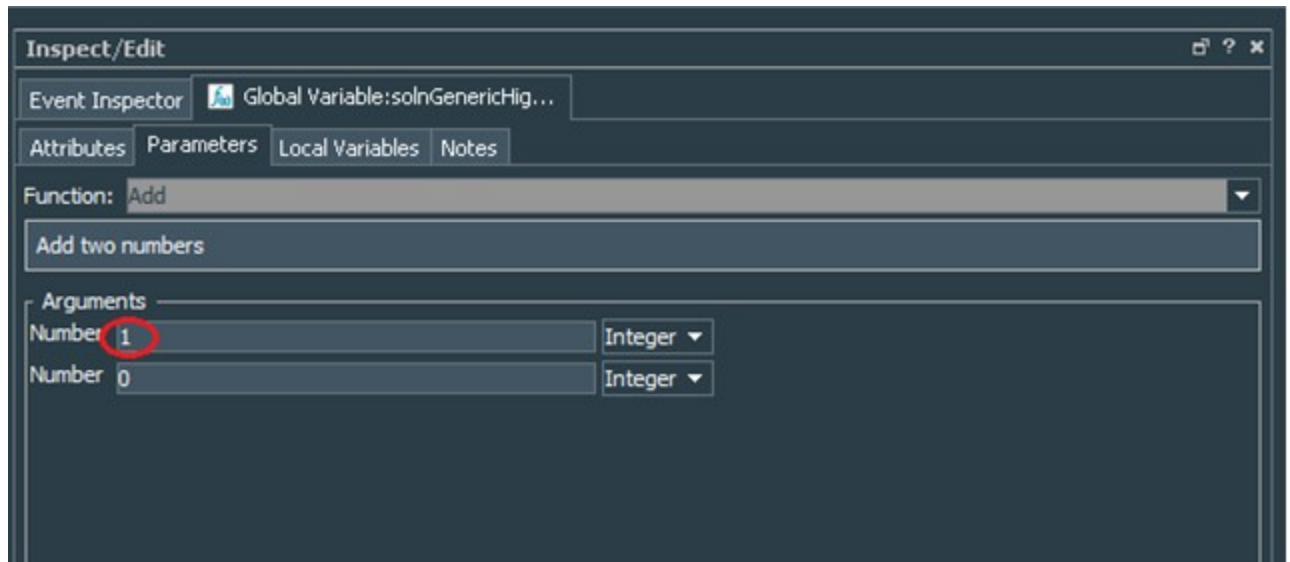
4. Click **OK** to save your changes.

Creating Custom Scenarios

In addition to the scenarios described in "RepSM Plus Scenarios" on page 11, you can
create custom scenarios for your organization. You first create a scenario rule and then
add the scenario name to the Scenarios active list. The custom scenarios will appear in
the Overview of Malicious Communication dashboard of the General Scenarios use
case.

To create a scenario rule:

1. Copy one of the RepSM Plus scenario rules; drag the rule from the `/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios` group and drop it in the same group.

2. Right-click the copied rule and select **Edit Rule**.

3. In the Inspect/Edit panel, modify the rule's condition and aggregation to match your
   scenario.

   If the situation detected by your scenario overlaps with other existing scenarios,
   multiple scenarios might be detected for the same base event.

4. On the Action tab, modify the following field as needed for your scenario:

- Device Custom String6 = *scenario name*

  Provide a descriptive name for the scenario. This is the name you will add to the Scenarios active list, and the name that will appear in the Overview of Malicious Communication dashboard. The name is case sensitive.

  The following fields are required; *do not modify them*:

  - Device Custom Number2 = **2**

  - Device Product = Reputation Security Monitor

5. On the Attributes tab, enter the scenario name in **Name** field.

   You can use any name for the rule, but for simplicity, use the same name for the both the rule and scenario.

6. Save the rule.

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

To add the scenario to the Scenarios active list:

1. From the Navigator panel Resources tab, select Lists from the drop-down list, and on the Active Lists tab, navigate to:

   `/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios`

2. Add the case-sensitive scenario name (that you specified in the Device Custom String6 field in the previous procedure) to the Scenarios active list.

   For information about adding an entry to an active list, see the *ArcSight Console User's Guide*.

When your rule triggers, you should see the events identified by your new scenario displayed in the Overview of Malicious Communication dashboard.

Enabling Trends

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

RepSM Plus includes trends, which are disabled by default. These disabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m. when network traffic is usually less busy than during peak daytime business hours.

These schedules can be customized to suit your needs using the Trend scheduler in the ArcSight Console.

To enable a trend:

> **Caution:** To enable a disabled trend, you must first change the default start date in the Trend editor.
>
> If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and backfills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

1. Go to the Navigator panel.
2. Right-click the trend you want to enable.
3. Select **Enable Trend**.

For more information about trends, refer to the following:

- The "Building Trends" topic in the *ArcSight Console User's Guide*.
- The Trends Best Practices document in Protect724.

Configuring Cases

Cases are a trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. Some RepSM Plus rules create a case if certain conditions are met. RepSM Plus includes the `All Cases/ArcSight Solutions/Reputation Security Monitor Plus` group, which holds the cases generated by some RepSM Plus rules.

You can add more groups to the `All Cases/ArcSight Solutions/Reputation Security Monitor Plus` group or add your own group if you want to add more differentiations. If you do add more groups, modify the rules that generate cases to use your new case groups.

For more important information about cases, see "Best Practices" on page 30.

Verifying RepSM Plus Content Configuration

After you have finished configuring the RepSM Plus content, you can use the Events Analyzed by RepSM Use Cases dashboard to see how many events have been

evaluated by each use case, and which devices generated those events. For more information, see "RepSM Package Health Status" on page 58.

Chapter 4: Using RepSM Plus Content

RepSM Plus provides the following use cases:

Best Practices

The following general recommendations apply to several of the RepSM Plus use cases.

Get Email About RepSM Plus Service Outages

A RepSM Plus service outage can affect the data displayed in several of the use case dashboards. Register for a Micro Focus Community Portal account so you can sign up to receive email notifications about such outages.

To receive emails, log in to the Security Community website and click the **Discussions** icon on the upper menu.

Navigate to **ArcSight User Discussion.** In the Filter by Labels section, select **RepSM**. Click **Subscribe** on the banner that will appear near the top of the page.

Service Notifications will be published to the ArcSight User Discussion forum using the RepSM label. By subscribing, you will automatically receive messages at your registered email.

Start With a Domain Name

Many of the RepSM Plus use case resources provide reputation data for either IP addresses or domain names. In general, IP addresses indicate clients, while domain names indicate servers. Domain names often include the name of the owning organization, which makes it easier to determine the source of an attack, investigate the attack, and contact the responsible party. You can often expedite your investigation by starting with a domain name.

Use the Integrated Web Search for Malicious Domains

Throughout the RepSM Plus use cases, you can get information about a malicious domains by right-clicking its name and selecting **Integration Commands > Search Selected Item in Google**.

For the following use cases, which detect outbound communication:

- Internal Infected Assets
- Dangerous Browsing

if the web search results indicate that the site is dangerous, find out whether the user of the internal asset has a valid reason to browse the site. Even if they do, you should inspect the internal asset for malware and take it offline if necessary.

If you think the site is not dangerous, consider deleting its entry from the Malicious Domains or Malicious IP Addresses active lists. To have the site removed more permanently from the reputation data, contact Customer Support. Alternatively, you can identify the site in an exception active list, as described in "Including and Excluding Entries from Reputation Data" on page 20.

Use Pattern Discovery in Your Investigation

Use the RepSM Plus Pattern Discovery profiles to find unknown patterns in your network–especially patterns that cannot be identified by any of the RepSM Plus scenario types. The profiles enable you to take graphic snapshots of patterns and then investigate further by using commands such as **Show related events**.

To get started, select Pattern Discovery in the Navigator panel, navigate to `All Profiles/ArcSight Solutions/Reputation Security Monitor Plus`, right-click a profile, and select **Take Snapshot**.

For detailed instructions on using Pattern Discovery, see the *ArcSight Console User's Guide*.

Sort Displays to Prioritize Your Investigation

Many of the use case tabular displays have column headings that indicate key information, such as the number of malicious hosts that communicated with an internal asset, or the number of interactions between a host and asset. Typically, the higher the number, the greater the risk. To help you decide which host or asset to investigate first, sort the display by clicking these column headings.

Dangerous Browsing

The Dangerous Browsing use case focuses on users who browse dangerous web sites. Dangerous browsing can happen intentionally when a user browses directly to an illegitimate web site, or unintentionally when a user follows malicious links on a legitimate web site. Dangerous browsing can also occur when a user is fooled by a phishing scheme, in which an illegitimate web site imitates a legitimate web site, usually with the intention of stealing credentials.

Although browsing dangerous web sites does not necessarily compromise your organization, such activities should be investigated and stopped because they can put the organization at legal risk, harm its reputation, and compromise security.

This use case detects outbound communications from internal assets, which are not public-facing, to malicious entities that have an exploit type of Phishing or Malware. The exploit types are configurable, as described in "Configuring Exploit Types" on page 21.

This use case does not open any cases.

Configuration:

Configure the Dangerous Browsing use case as follows for your environment:

- Optional, but recommended. Categorize your organization's public assets (those that are accessible from the internet) as Public-Facing. This reduces the number of unintended events detected by the use case and helps eliminate false positives.

  For more information, see "Categorizing Assets" on page 22.
- Optional. Set the reputation score threshold in the rules used by the use case.

  You can set different thresholds for the domain names and IP addresses. By default, the thresholds are set to 1, so reputation scores from 1 to 100 are considered. The thresholds are set in the following global variables:
  - Dangerous Browsing Reputation IP Score Threshold
  - Dangerous Browsing Reputation Domain Score Threshold

For details, see "Setting Thresholds for the Reputation Score" on page 25.

- Optional. Add entries to the Dangerous Browsing Exploit Types active list. By default, the use case detects:

  - Outbound communications to malicious hosts that have an exploit type of Phishing or Malware.

  - Ad fraud

  - Compromised & Links to Malware

  - Malware

  - Malware-Call Home

  - Malware Distribution Point

  - Phishing

  - Phishing/Fraud

  You can add additional exploit types to the active list. For a list of exploit types, see "Exploit Types" on page 10.

  For details about adding entries to an active list, see "Configuring Exploit Types" on page 21.

- Optional. Define your own reputation data by adding entries to the active lists described in "Including and Excluding Entries from Reputation Data" on page 20.

To use the Dangerous Browsing use case:

This section describes a likely scenario for investigating users browsing to dangerous web sties and highlights some key features of the use case.

1. Click the **Use Cases** tab in the Navigator panel and open the **Dangerous Browsing** use case located in:

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security
   Monitor Plus
   ```

   The overview dashboard is a good starting point for your investigation.

2. Open the Overview of Dangerous Browsing dashboard.
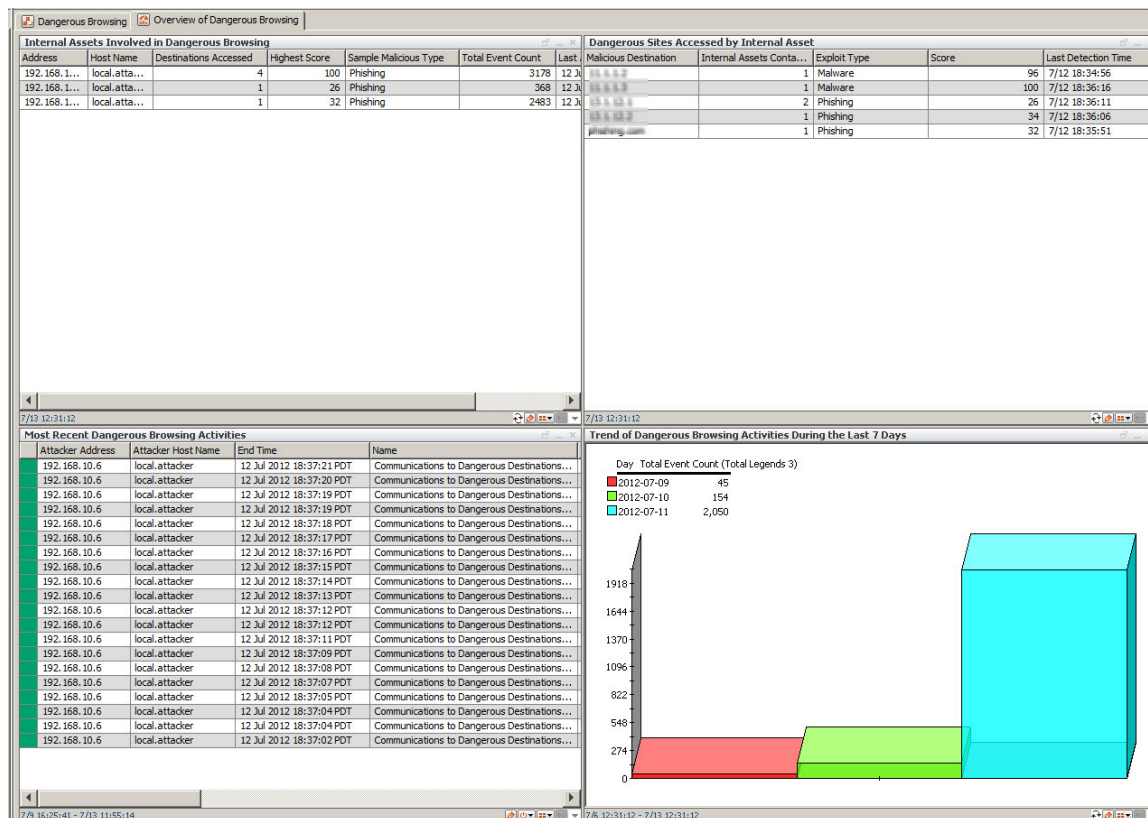
3. Review the information in the Internal Assets Involved in Dangerous Browsing component on the dashboard.

4. Double-click an internal asset to display its dangerous browsing activities.

5. In the resulting display, double-click an asset to display the base events that involved this asset during the last 24 hours.

6. In the resulting display, right-click an event and select **Investigate > Show Simple Rule Chain** to show both the correlation even and the base event in the Event Inspector. This provides additional event fields and values that are not shown in the query viewer.

7. Return to the overview dashboard and open the **Dangerous Sites Accessed by Internal Asset** component.

8. To get more information about a dangerous site, right-click its name and select **Integration Commands > Search Selected Item in Google**. (You can use this command in most of the RepSM use cases.)

   If the search results indicate the site is dangerous, find out whether the user of the internal asset has a valid reason to browse the site. Even if they do, you should inspect the internal asset for malware and take it offline if necessary.

   If you think the site is not dangerous, consider deleting its entry from the Malicious Domains or Malicious IP Addresses active lists. To have the site removed more permanently from the reputation data, contact Customer Support.

9. Return to the use case tab to review the other resources in the use case.

    You can run reports that provide stakeholders with information about current and long term dangerous browsing.

Key Resources

The following tables list the key resources in this use case that might require configuration or that you might use during your investigation.

Monitor Resources that Support the Dangerous Browsing Use Case

Resource	Description	Type	URI
Overview of Dangerous Browsing	This dashboard shows an overview of all dangerous browsing activities and access to dangerous destinations. You can drilldown to get to more information about the related destinations and the base events.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities - One Year Trend	This report provides information about dangerous browsing activities by internal assets during the last year.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities During the Last 7 Days	This report provides information about dangerous browsing activities by internal assets during the last seven days.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities During the Last 24 Hours - Short Form	This report provides information about browsing activities by internal assets to malicious destinations during the last 24 hours. It shows less data than the longer counterpart.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities - 30 Day Trend	This report provides information about dangerous browsing activities by internal assets during the last 30 days.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities During the Last 24 Hours - Long Form	This report provides information about browsing activities by internal assets to malicious destinations during the last 24 hours.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/

Library Resources that Support the Dangerous Browsing Use Case

Resource	Description	Type	URI
Dangerous Browsing Exploit Types	This active list contains all exploit types considered as dangerous browsing. By default, it contains Malware and Phishing.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Dangerous Browsing Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Dangerous Browsing use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/
Dangerous Browsing Reputation Domain Score Threshold	This variable stores the score threshold for malicious domain names used in the Dangerous Browsing use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/

General Scenarios

The General Scenarios use case provides resources that focus on inbound and outbound malicious communication identified by scenarios.

For a detailed comparison of the scenarios provided with RepSM Plus, see "RepSM Plus Scenarios" on page 11 . For information about creating your own scenarios, see "Creating Custom Scenarios" on page 26.

Configuration:

This is optional. If you created any custom scenarios, add them to the Scenarios active list as described in "Creating Custom Scenarios" on page 26.

To use the General Scenarios use case:

1. Click the **Use Cases** tab in the Navigator panel and open the **General Scenarios** use case located in:

   ```
   All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus
   ```

2. Open the Overview of Malicious Communication dashboard.

   The dashboard shows an overview of all malicious inbound and outbound communication events, broken down by scenarios such as Port Scan or Potential Intrusion.
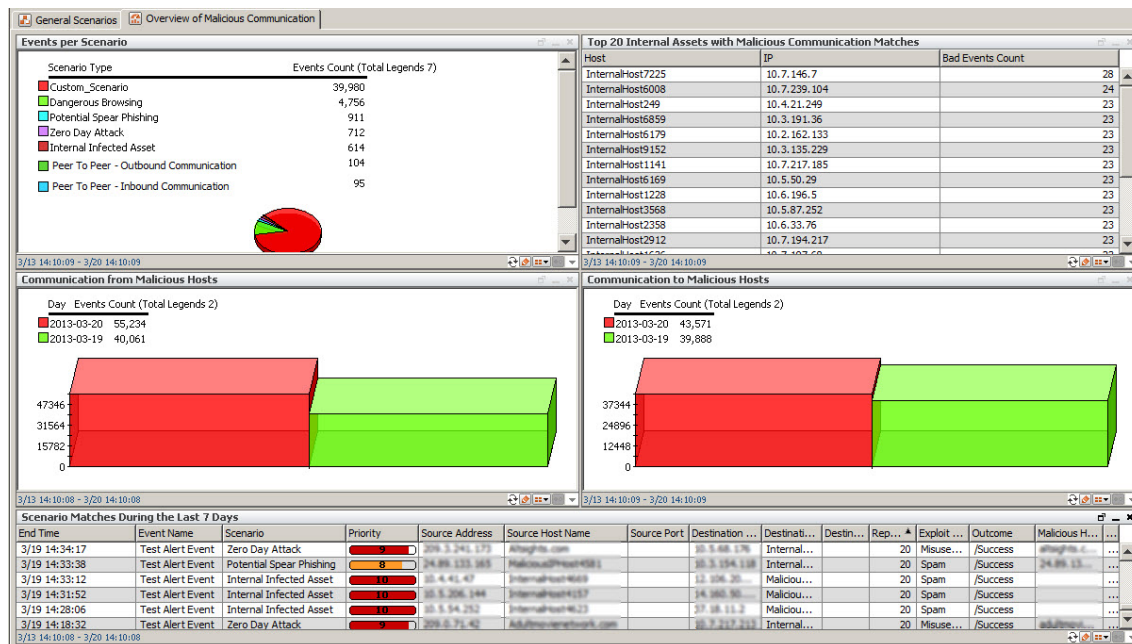
3. The upper right component shows the top 20 internal assets with most the malicious communication. Right-click a row and use the drilldown commands to filter malicious communication by he IP address or host name.

4. The lower component shows all of the events identified by a scenario during the last seven days. Right-click a row and use the drilldown commands to apply different filters to the events.

Key Resources

The following tables list the key resources in this use case that might require configuration or that you might use during your investigation.

Monitor Resources that Support the General Scenarios Use Case

Resource	Description	Type	URI
Malicious Communication Matches Recently	This active channel displays all malicious communication match events during the last 2 hours.	Active Channel	/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Overview of Malicious Communication	This dashboard shows an overview of all malicious inbound and outbound communication events.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

Monitor Resources that Support the General Scenarios Use Case, continued

Resource	Description	Type	URI
Scenario Matches During the Last 7 Days	This query viewer shows all events related to scenario types captured during the last seven days.	Query Viewer	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Malicious Communication Matches During the Last 7 Days	This query viewer shows all malicious inbound and outbound communication events during the last seven days, in tabular format.	Query Viewer	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Inbound and Outbound Malicious Communication during the Last 7 Days	This report shows detailed information about events with malicious communication during the last seven days.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
List of Internal Assets with Malicious Communication during the last 7 Days	This report shows information about all internal assets with malicious communication during the last seven days.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Malicious Communication Trend over Time of the Last Day	This report shows an overview of captured malicious communication during the last day, and shows the Inbound and Outbound trends over time and the scenario events captured. The report includes communication from malicious hosts during the last day in a bar chart, communication to malicious hosts during the last day in a bar chart, and scenario type events during the last day in tabular format.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Events for which a Scenario was Identified	This report shows detailed information about all scenario matches during the last seven days. The information includes the event count per scenario during the last day in a pie chart and all the captured Scenario events during the last seven days in tabular format.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

Library Resources that Support the General Scenarios Use Case

Resource	Description	Type	URI
Scenarios	This active list maintains a list of the scenarios presented by General Use Case Scenarios. The Scenario Name field is compared against the Device Custom String6 field of the event.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

RepSM Plus Overview

The RepSM Plus Overview use case provides quick access to the overview dashboards provided by the other RepSM Plus use cases, and is especially helpful if you are unfamiliar with the RepSM Plus content.

Configuration:

This use case does not require additional configuration.

To use the RepSM Plus Overview use case:

1. Click the **Use Cases** tab in the Navigator panel and open the **RepSM Overview** use case located in:

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security
   Monitor Plus
   ```

2. Open the **RepSM Plus Overview** dashboard.

   The dashboard provides a high-level, consolidated view of issues based on threat intelligence. It provides an overview of traffic from reputation hosts in the last 24 hours (not real time).
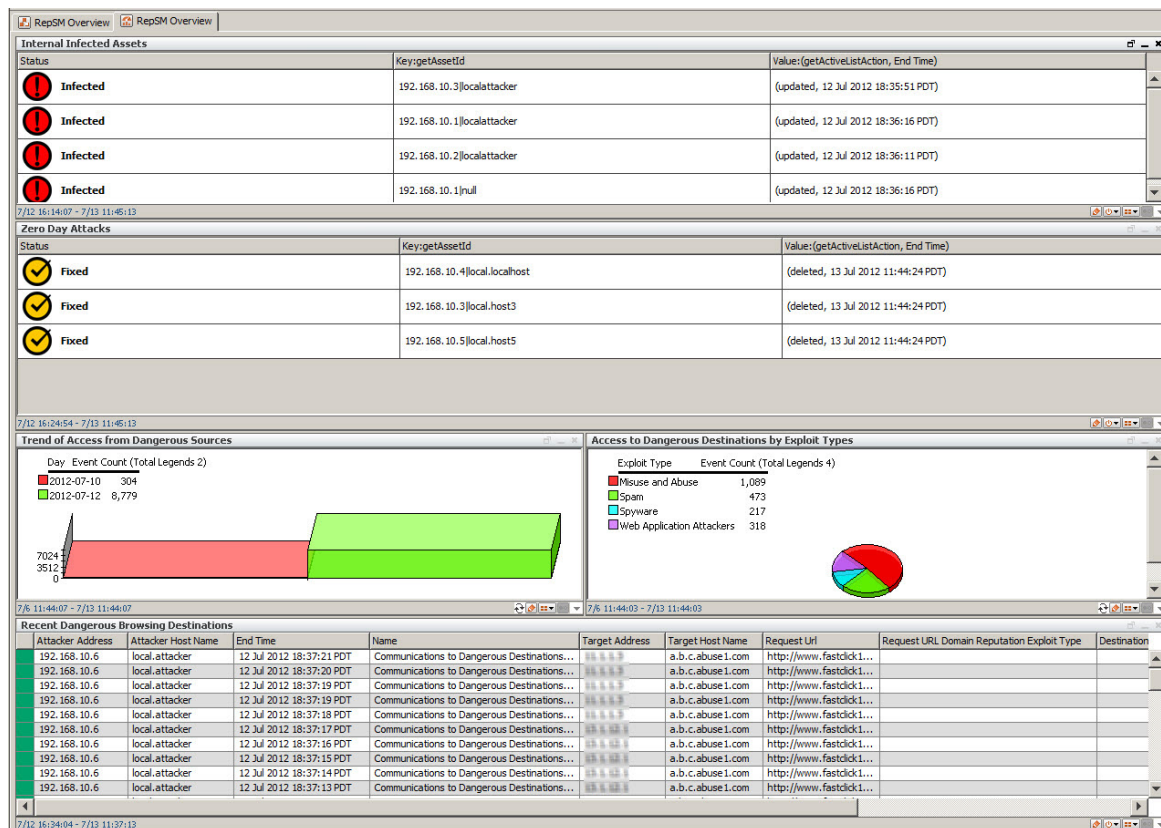
By using drilldowns, you can move from this dashboard to other use case dashboards for increasingly detailed information–including exploit types, reputation scores, detection times, attack counts, and event counts–and then finally to the base events that caused an asset to appear on the dashboard.

3. Right-click any component and select **Drilldown > Overview of**... to display the overview dashboard for the use case. For more information about the overview dashboards, see the section for that use case in the remainder of this chapter.

   (To enable the drilldown in the data monitors at the top of the dashboard, you might need to click the AssetID in a row before right-clicking.)

4. Return to the use case tab and open the **Geographical View of Malicious Communications** dashboard to see a map of malicious communication. Use the tabs at the bottom of the map to show either access to or attacks from malicious entities.
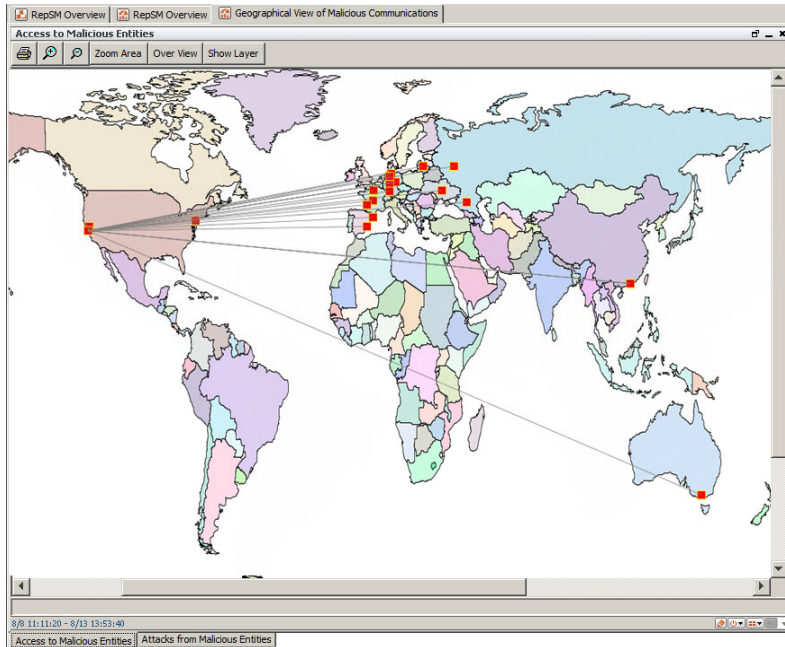
Internal Infected Assets

The Internal Infected Assets use case helps protect from Advanced Persistent Threat (APT) attacks by identifying internal assets that attempted to communicate with a command and control center, or a member of a botnet. Even if the communication attempt failed, the attempt itself indicates that malicious software might exist on the asset.

For more information, see "Protect from Advanced Persistent Threats (APTs)" on page 8.

This use case provides information about internal assets that are either:

- Public-facing and communicating with a malicious entity, regardless of its exploit type. These assets are typically servers that do not normally initiate outbound communication, so initiating communication with a malicious entity is of particular interest.
- Not public-facing and communicating with a malicious entity that has an exploit type of Botnet. These assets might be participating in a botnet network.

The exploit types are configurable, as described in "Configuring Exploit Types" on page 21.

> Note: This use case opens a case for every detected internal infected asset. For important information about cases, see "Best Practices" on page 30.

Configuration:

Configure the Internal Infected Assets use case as follows for your environment:

- Optional, but recommended. Categorize your organization's public assets (those that are accessible from the internet) as Public-Facing.

  For more information, see "Categorizing Assets" on page 22.

- Optional. Add entries to the Critical Exploit Types active list. By default, the use case identifies:

  - Communications to malicious hosts that have an exploit type of Botnet.
  - Compromised and links to malware
  - Spyware and questionable software

  For a list of exploit types, see "Exploit Types" on page 10.

  For details about adding entries to an active list, see "Configuring Exploit Types" on page 21.

  - Optional. Add entries to the Critical Exploit Types active list. By default, the use case identifies:

    - Communications to malicious hosts that have an exploit type of Botnet.
    - Compromised and links to malware
    - Spyware and questionable software

    For a list of exploit types, see "Exploit Types" on page 10.

    For details about adding entries to an active list, see "Configuring Exploit Types" on page 21.

- Optional. Set the reputation score threshold in the rules used by the use case.

  You can set different thresholds for the domain names and IP addresses. By default, the thresholds are set to 1, so reputation scores from 1 to 100 are considered. The thresholds are set in the following global variables:

  - Internal Infected Assets Reputation IP Score Threshold
  - "Internal Infected Assets Reputation Domain Score Threshold" on page 46

    For details, see "Setting Thresholds for the Reputation Score" on page 25.

- Optional. Define your own reputation data by adding entries to the active lists described in "Including and Excluding Entries from Reputation Data" on page 20.

To use the Internal Infected Assets use case:

This section describes a likely scenario for investigating internal infected assets and highlights some key features of the use case.

1. Click the Use Cases tab in the Navigator panel and open the Internal Infected Assets use case located in:

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security
   Monitor Plus
   ```

   Review the resources provided by the use case. The overview dashboard is a good starting point for your investigation.

2. Open the Overview of Internal Infections dashboard. Each component on the dashboard provides a different aspect of the infected assets detected by this use case.
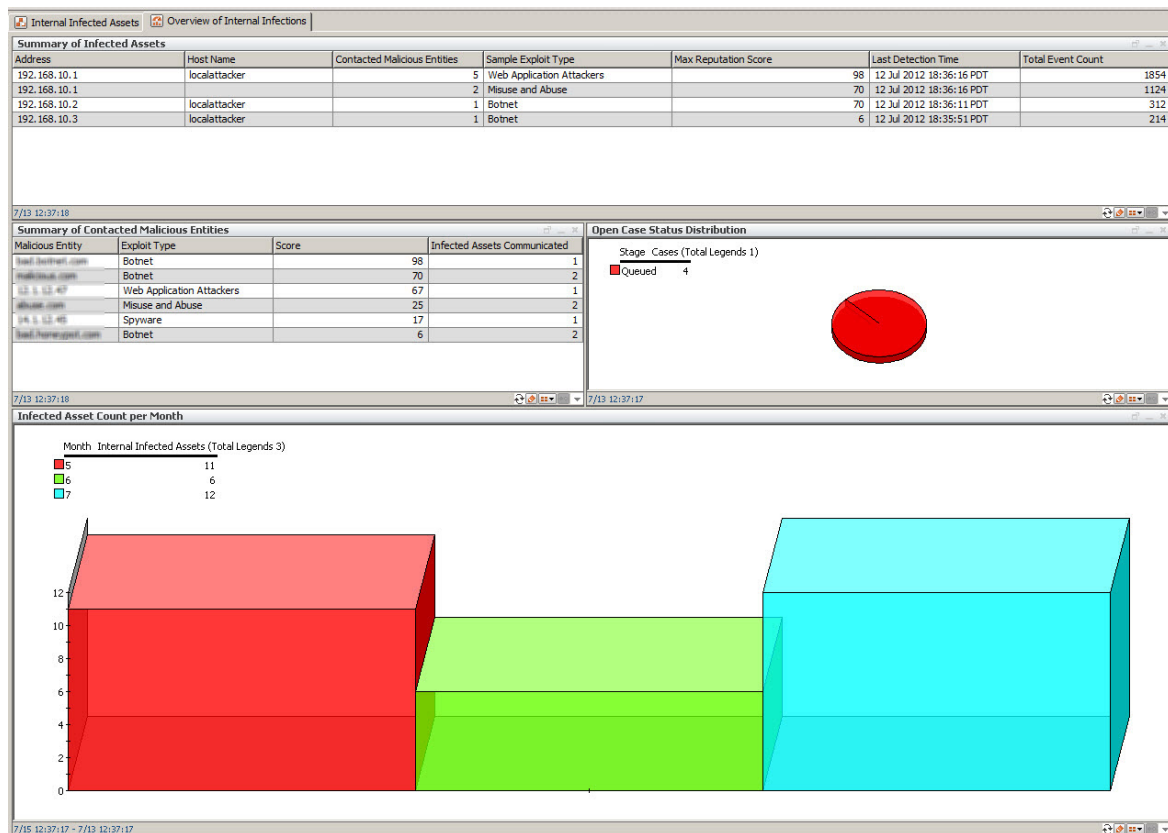
3. Review the information in the Summary of Infected Assets component on the dashboard. The internal assets in this list are assumed to be infected by potentially dangerous malware and should be investigated immediately.

   > **Tip:** To help prioritize your investigation, sort the display by clicking the **Contacted Malicious Entities** column heading. Typically, the higher the number, the greater the risk.

4. Double-click an infected asset to display additional information, including the command and control centers or botnet servers the asset tried to contact.

   From this display, several drilldown options are available to investigate the infection further, down to the base event level.

5. Right-click an asset and select Drilldown to see the options. You can drill down to:

   - the base events that represent direct communication with a malicious entity

   - other internal assets that might have been infected by the infected asset

   - all inbound and outbound communications with the infected asset, which might reveal other possible malicious entities

6. Select any of the drilldowns to display the events associated with the infected asset.

7. In the resulting display, right-click a row and select **Investigate > Show Event Details** to show the base event in the Event Inspector. This provides additional event fields and values that are not shown in the query viewer.

8. Return to the overview dashboard and examine the other components.

   The Summary of Contacted Malicious Entities component focuses on command and control centers that the internal asset contacted. Double-click a malicious entity to see which assets have communicated with it and then use the drilldowns to continue your investigation, as described in previous steps.

9. A case is opened for every detected internal infected asset. The Open Case Status Distribution component on the overview dashboard shows the status of these cases. Click the pie chart to display detailed information about the cases.

   For more information about cases, see .

10. Return to the use case tab to review the other resources in the use case.

    You can run reports that provide stakeholders with information about current and long term asset infections. You can use the active channels to see real time events to and from infected assets.

Key Resources

The following tables list the key resources in this use case that might require configuration or that you might use during your investigation.

Monitor Resources that Support the Internal Infected Assets Use Case

Resource	Description	Type	URI
All Interactions with Malicious Entities Detected During the Last 2 Hours	This active channel shows all the occurrences of rules that triggered to detect internal infections in this use case in the last two hours.	Active Channel	/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Events To or From Infected Assets During the Last 2 Hours	This active channel shows all events to or from the infected machines in the last two hours.	Active Channel	/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Overview of Internal Infections	This dashboard provides an overview of internal infected assets, including hosts that are communicating with external malicious entities, and the trend of infections over time. You can drilldown from the summary query viewers to specific interactions or base events.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Overview of Infected Assets During the Last 30 Days	This report shows an overview of internal infections over the last one month (up to and including yesterday). Its content is based on a daily trend which stores the daily snapshot of the Infected Internal Assets active list.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Assets Infected for More Than A Week	This report shows all infected internal machines that have remained in the infection list for over one week. This might mean that the related cases have not yet been investigated or are still being investigated. By default, when a case on internal infection asset is deleted or closed, the related asset will be removed from the infection list.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Currently Infected Assets and Recorded Interactions with Malicious Entities	This report shows the internal assets that are considered to be infected through their communications with external malicious hosts.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Interactions with Malicious Entities During the Last 24 Hours	This report shows all interactions with certain malicious entities by internal assets. These assets are then considered infected. Note that an internal asset might be involved in multiple interactions, depending on its communications, but will be reported under a single case.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/

Library Resources that Support the Internal Infected Assets Use Case

Resource	Description	Type	URI
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Public-Facing	This is a solutions asset category.	Asset Category	/All Asset Categories/ArcSight Solutions/Reputation Security Monitor Plus
Internal Infected Assets Reputation Domain Score Threshold	This variable stores the score threshold for reputation domain names used in the Internal Infected Assets use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/
Internal Infected Assets Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Internal Infected Assets use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/

Zero Day Attacks

The Zero Day Attack use case helps detect attacks that exploit previously unknown vulnerabilities in software – before vendors of security software, such as antivirus, IDS, and IPS, have time to address the vulnerability. This use case attempts to detect such compromises if they originate from malicious IP addresses or domains. The use case identifies successful communication to internal, non-public facing assets from external malicious entities that have an exploit type of Botnet, Misuse and Abuse, Miscellaneous, Web Application Attacker, and Worm.

The exploit types are configurable, as described in "Configuring Exploit Types" on page 21.

Note: This use case opens a case for every detected asset that is the target of a zero day attack. For important information about cases, see "Best Practices" on page 30.

Configuration:

Configure the Zero Day Attacks use case as follows for your environment:

- Required. Categorize the assets in your organization that are not public-facing (those that are not accessible from the internet) as Internal Non Public-Facing.

  For more information, see "Categorizing Assets" on page 22.

- Optional. Add entries to the Zero Day Attack Exploit Types active list. By default, the use case identifies:
  - Communications to malicious hosts that have an exploit type of Botnet, Misuse and Abuse, Miscellaneous, Web Application Attacker, and Worm.
  - Command and Control Centers
  - Spyware and Questionable Software

  You can add additional exploit types to the active list. For a list of exploit types, see "Exploit Types" on page 10.

  For details about adding entries to an active list, see "Configuring Exploit Types" on page 21.
- Optional. Set the reputation score threshold in the rules used by the use case. These thresholds determine the minimum reputation score to track and report zero day attacks.

  You can set different thresholds for the domain names and IP addresses. By default, the thresholds are set to 1, so reputation scores from 1 to 100 are considered. The thresholds are set in the following global variables:
  - Zero Day Attacks Reputation Domain Score Threshold
  - Zero Day Attacks Reputation IP Score Threshold

  For details, see "Setting Thresholds for the Reputation Score" on page 25.
- Optional. Define your own reputation data by adding entries to the active lists described in "Including and Excluding Entries from Reputation Data" on page 20.

To use the Zero Day Attacks use case:

This section describes a likely scenario for investigating zero day attacks and highlights some key features of the use case.

1. Click the Use Cases tab in the Navigator panel and open the Zero Day Attacks use case located in:

   ```
   All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus
   ```

   The overview dashboard is a good starting point for your investigation.
2. Open the Overview of Zero Day Attacks dashboard. Each component on the dashboard provides a different aspect of the infected assets detected by this use case.
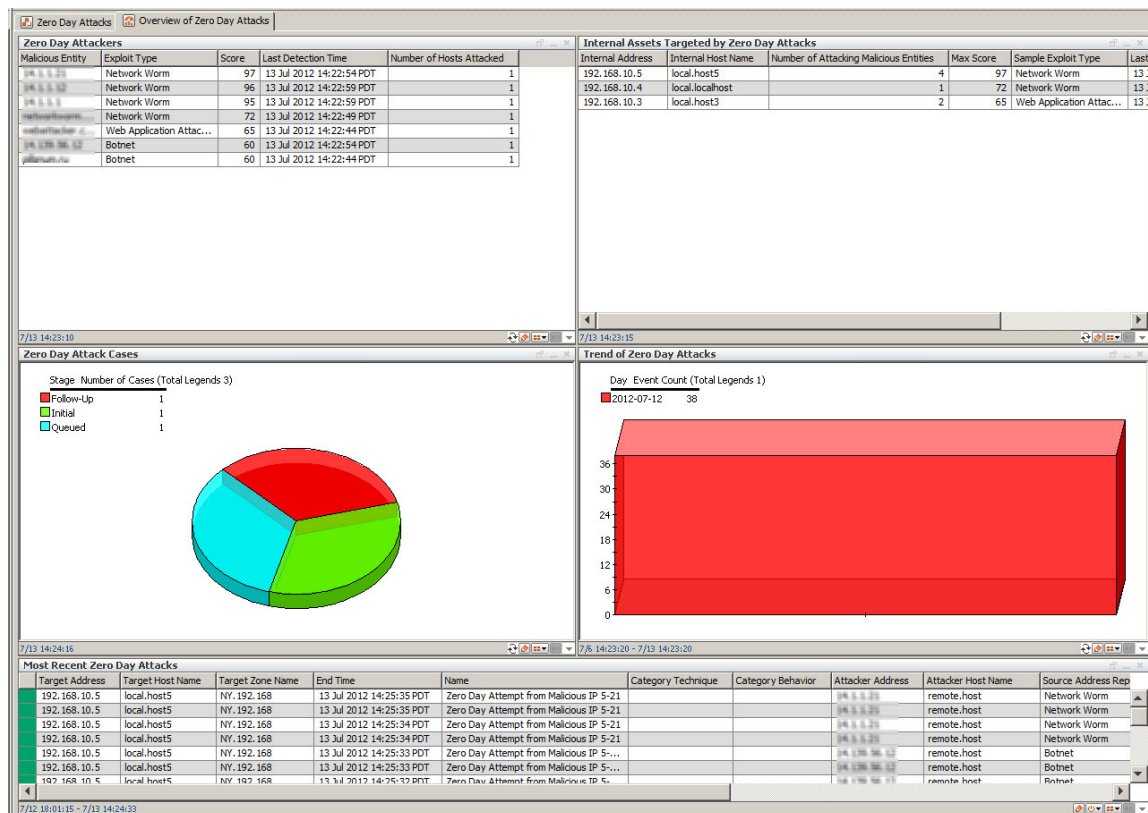
3. Review the information in the Internal Assets Targeted by Zero Day Attacks component on the dashboard. The internal assets in this list are assumed to have been attacked by zero day exploits and should be investigated immediately.

4. Double-click an attacked asset to display additional information about the attacker.

5. In the resulting display, double-click an attacked asset to see the events involved in the attack.

6. In the resulting display, right-click a row and select **Investigate > Simple Rule Chain** to show both the correlation event and the base event in the Event Inspector. This provides additional event fields and values that are not shown in the query viewer.

7. Return to the overview dashboard and examine the other components.

   You can use the Zero Day Attackers component to begin your investigation with the attacker, rather than the internal asset. Double-click a malicious entity to see which assets it has communicated with and then use the drilldowns to continue your investigation.

8. A case is opened for every detected zero day attack. The Zero Day Attack Cases component on the overview dashboard shows the status of these cases. Click the pie chart to display detailed information about the cases.

   For more information about cases, see "Best Practices" on page 30.

9. Return to the use case tab to review the other resources in the use case.

You can run reports that provide stakeholders with information about current and long term asset infections. You can use the active channels to see real time events to and from infected assets.

Key Resources

The following table lists the key resources in this use case that might require configuration or that you might use during your investigation.

Resources that Support the Zero Day Attacks Use Case

Resource	Description	Type	URI
Overview of Zero Day Attacks	This dashboard shows an overview of all zero day attacks. You can drilldown to more information about the related sources and targets and the base events.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks During the Last 7 Days	This report provides information about zero day attacks on internal assets during the last seven days. Do not change the default value for the custom parameter AttackType.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks During the Last 24 Hours	This report provides information about zero day attacks to internal assets during the last 24 hours.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks - One Year Trend	This report provides information about zero day attacks to internal assets during the last year. Do not change the default value for the custom parameter AttackType.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks - 30 Day Trend	This report provides information about zero day attacks by malicious entities on internal assets during the last 30 days. Do not change the default value for the custom parameter AttackType.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/

Library Resources that Support the Zero Day Attacks Use Case

Resource	Description	Type	URI
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant to zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, and Miscellaneous.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	/All Asset Categories/ArcSight Solutions/Reputation Security Monitor Plus
Zero Day Attacks Reputation Domain Score Threshold	This variable stores the score threshold for malicious domain names used in the Zero Day Attacks use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/
Zero Day Attacks Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Zero Day Attacks use case.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/

Internal Assets Found in Reputation Data

The Internal Assets Found in Reputation Data use case helps ensure the reputation of your organization's assets by detecting when those assets appear in the reputation database. This situation can indicate that assets have been compromised and are being used for malicious purposes. However, even if an asset is wrongly included in the database, it should be investigated to avoid issues such as email from your organization being marked as spam. You can also use this use case to detect when the assets of trusted partners and suppliers appear in the reputation database.

> **Note:** This use case opens a case for every detected asset found in the reputation data. For important information about cases, see .

Configuration:

This use case relies on queries or active lists, which must be configured with domain names and IP addresses as described below.

- Specify the domain names to monitor.

  The Internal Domain Reputation Detector hourly trend detects domain names in the reputation database. You can specify those domain names in either a query or an active list, depending on how many domain names you need to monitor.

  ○ If you have only a few domains to monitor, specify the domain names directly in the Internal Domain Reputation Detector (List Based) - Trend Base query.

  ○ Edit the query and specify each domain name by using the Domain condition. The query contains a sample condition, which you can copy and change as needed. For example, you might specify `Domain endsWith .xyzCompany.com`.

  ○ If you have many domains to monitor, add the domain names to the Internal Internal Domains for Reputation Monitoring active list. Specify the second-level and third-level domains that represent your organization, for example, microfocus.com or microfocus.co.uk

    For details, see "Configuring Internal Assets Found in Reputation Data" on page 22.

- Specify the IP addresses to monitor.

  If the IP addresses are already represented as assets in ArcSight ESM or ESM Express, no configuration is needed. RepSM Plus captures all the assets whose IP addresses are found in the reputation database. For information about modeling your network assets, see *ESM 101* and *ArcSight Console User's Guide*.

  If the IP addresses are not represented as assets, or if you want to monitor a range of IP addresses, or a subnet, configure the Internal Asset Reputation Detector (List Based) - Trend Base query listed in "Reputation Security Monitor Plus Resource Reference" on page 69.

  The query contains sample conditions for several types of addresses:

  ○ A network address in Classless Inter-Domain Routing (CIDR) format: 192.0.2.0-192.0.2.255

  ○ A specific network address prefix: 198.51.100.0

  ○ A class A, B, or C network address, which you specify in the Internal Network Addresses for Reputation Monitoring active list.

  ○ A specific IP address, which you specify in the Internal Assets for Reputation Monitoring active list.

Determine which conditions best suit your network environment and then specify the addresses either directly in the query or in the active lists.

> **Tip:** To minimize the overhead associated with the query, delete the conditions that you do not use.

To use the Internal Assets Found in Reputation Data use case:

1. Click the **Use Cases** tab in the Navigator panel and open the **Internal Assets Found in Reputation Data** use case located in:

   `/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus`

2. Review the resources provided by the use case.

3. Open the Internal Assets and Domains Found in Reputation Data dashboard.

4. Right-click a domain name, host name, or IP address and use the drilldowns to show the events to or from the asset within the last 24 hours.

5. A case is opened for every internal asset found in the reputation database. You can access the cases from the Navigator panel Resources tab, by selecting **Cases** from the drop-down list and navigating to:

   `/All Cases/ArcSight Solutions/Reputation Security Montior Plus/Internal Assets Found in Reputation Data`

   To simplify your investigation, the case name includes the IP address or domain name of the asset. Open a case and click the **Events** tab to see the events associated with the asset.

   For more information about cases, see "Best Practices" on page 30.

6. Return to the use case tab to review the other resources in the use case.

You can run a report that provides stakeholders with information about the internal assets found in the reputation database.

> **Note:** If you think an asset should not be included in the reputation database, consider deleting its entry from the Malicious Domains or Malicious IP Addresses active lists. However, the next time the data is refreshed by the Model Import Connector for RepSM Plus, the asset might reappear in the active lists. To remove the asset more permanently, contact Customer Support.

Key Resources

The following tables list the key resources in this use case that might require configuration or that you might use during your investigation.

Monitor Resources that Support the Internal Assets Found in Reputation Data Use Case

Resource	Description	Type	URI
Internal Assets and Domains Found in Reputation Data	This dashboard provides information around internal assets or domain names reported in the reputation database.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Assets Found in Reputation Data	This report shows the list of internal IP addresses and internal domain names found in reputation data.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

here

Library Resources that Support the Internal Assets Found in Reputation Data Use Case

Resource	Description	Type	URI
Internal Domains for Reputation Monitoring	This active list contains the domain names to be monitored for existence in the reputation database. The domain names in this list should be just the top two or three levels, such as microfocus.com or microfocus.co.uk.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Network Addresses for Reputation Monitoring	This active list stores all local public network addresses (only class A, B or C) to be monitored for existence in the reputation database. If your network does not use these classes (for example, it uses CIDR instead), you can use the smallest class that fully represents your network. For example, a network address of 192.168.1.1/26 can be represented by a class C network of 192.168.1.0, so you can put 192.168.0. in this list. Note that for each network address entry , a dot (.) character is required.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Assets for Reputation Monitoring	This active list stores the addresses of all local assets that need to be monitored for existence in the reputation database.	Active List	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Domain Reputation Detector (List Based) - Trend Base	This query returns all internal domain names that appear in the reputation domain database. It runs on top of the reputation domain database and correlates with the specified domain names.	Query	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Asset Reputation Detector (List Based) - Trend Base	This query returns all internal hosts that appear in the reputation IP database. It runs on top of the reputation IP database and correlates with the assets to be monitored, as defined in an active list.	Query	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Event Enrichment with Reputation Data

The Event Enrichment with Reputation Data use case provides resources that let you add reputation data to non-RepSM Plus resources. By enriching those resources with global threat intelligence, security analysts can focus on key events involving known malicious entities.

No configuration is required for this use case.

To use the Event Enrichment with Reputation Data use case:

You can enrich your existing ArcSight resources with data about malicious entities to provide better context when investigating an incident. The global variables described in the Key Resources table below provide that data and can be included in all ArcSight resources.

For example, you can enhance an existing active channel, which you already use to monitor suspicious events from an IDS, to include information such as whether the attacker is a known malicious host, and if so, the attacker's reputation score and exploit type. To do so, you could add the following global variables to the active channel's field set:

- RepSM Product
- Source Domain Reputation Score
- Destination Domain Reputation Exploit Type

This is just one example; for a description and the location of these and other variables, see the Key Resources table.

For more information about global variables, see the *ArcSight Console User's Guide*.

Key Resources

The following tables list the key resources in this use case that might require configuration or that you might use during your investigation.

Library Resources that Support the Event Enrichment with Reputation Data Use Case

Resource	Description	Type	URI
Destination Domain Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) host name based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Destination Address Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) IP based on the reputation IP data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Destination Address Reputation Score	This variable returns the reputation score of a malicious target (or a destination) host name based on the reputation IP data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/

Library Resources that Support the Event Enrichment with Reputation Data Use Case, continued

Resource	Description	Type	URI
Source Reputation Domain	This variable returns the reputation domain (or host name) related to a malicious attacker (or source) host name based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Domain Reputation Score	This variable returns the reputation score of a malicious attacker (or a source) host name based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Address Reputation Exploit Type	This variable returns the exploit type of a malicious attacker (or a source) IP address based on the reputation IP data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Domain Reputation Exploit Type	This variable returns the exploit type of a malicious attacker (or a source) host name based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
RepSM Product	This global variables returns Reputation Security Monitor for events with reputation information. Otherwise, it returns the original Device Product.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Address Reputation Score	This variable returns the reputation score of a malicious attacker (or a source) host name based on the reputation IP data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Request URL Domain Reputation Score	This variable returns the score of a domain from a URL request based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Destination Domain Reputation Score	This variable returns the reputation score of a malicious target (or a destination) address based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/

Library Resources that Support the Event Enrichment with Reputation Data Use Case, continued

Resource	Description	Type	URI
Request URL Reputation Domain	This variable returns the reputation domain from a URL request based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Request URL Domain Reputation Exploit Type	This variable returns the exploit type of a domain from a URL request based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Destination Reputation Domain	This variable returns the reputation domain related to a malicious target (or destination) host name based on the reputation domain data.	Global Variable	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Request URL Enrichment	This field set contains fields with reputation information (based on the request URL) for event enrichment purposes.	Field Set	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Reputation IP Enrichment	This field set contains fields with reputation IP information for event enrichment purposes.	Field Set	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Reputation Domain Enrichment	This field set contains fields with reputation domain information for event enrichment purposes.	Field Set	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Events to Malicious Targets	This filter identifies events whose targets are found in the reputation database.	Filter	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/
Events from Malicious Sources	This filter identifies events whose attackers are found in the reputation database.	Filter	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/
Events with Requests to Malicious Hosts	This filter identifies events with requests to hosts found in the reputation database.	Filter	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/
RepSM Relevant Events	This filter identifies events that contains information related to reputation data (for example, host address or request URL).	Filter	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/

RepSM Package Health Status

The RepSM Plus Package Health Status use case provides information about the operational status of important RepSM Plus resources. Various dashboards show the state of important rules and trends; the number of events evaluated by each RepSM Plus use case and the devices that generated those events; and messages from the Model Import Connector for RepSM Plus and the RepSM Plus service.

For an explanation of RepSM Plus service messages, see "RepSM Plus Activation Messages" on page 1.

With the new dashboard, alerts are triggered by the RepSM Plus service outage or whenever intelligent data is not received or processed in a certain period.

Make sure that the TTL of /All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Track RepSM MIC is correct.

By default, data syncs every two hours, as a result, its TTL is 2:05 hour. If interval is modified, for example, it is modified to 1 hour, the TTL should be changed to 1:05, as well.

To use the RepSM Package Health Status use case:

1. Click the **Use Cases** tab in the Navigator panel and open the **RepSM Package Health Status** use case located in:

   ```
   /All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus
   ```

2. Open the Events Analyzed by RepSM Use Cases dashboard.
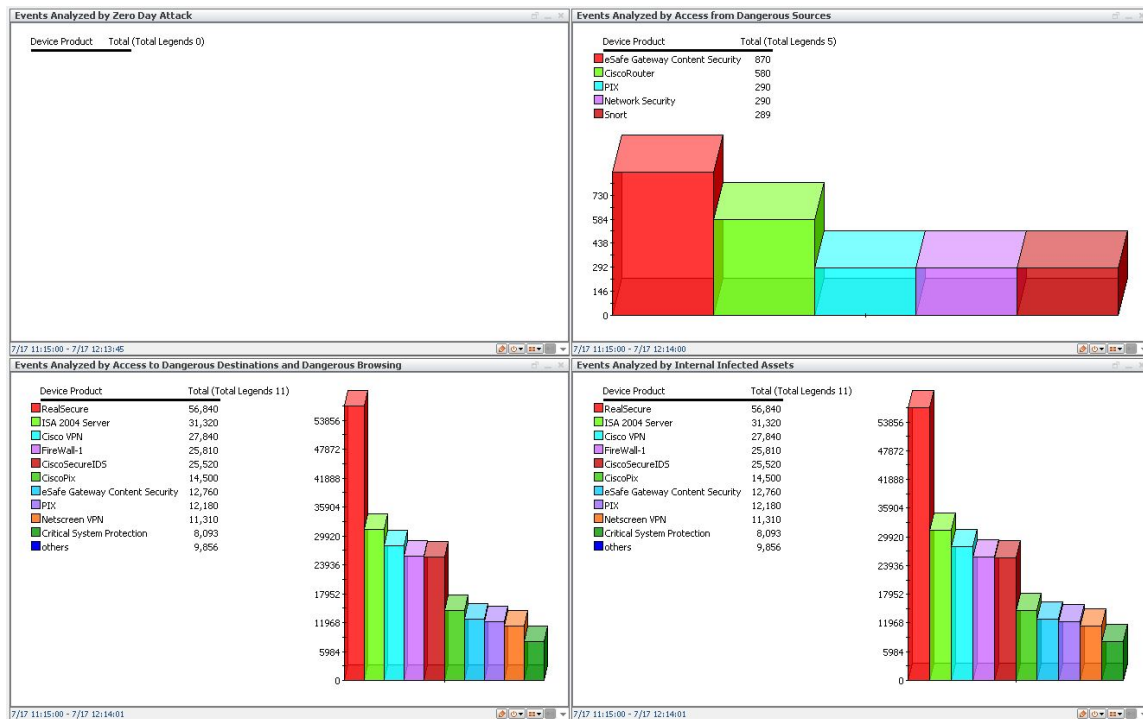
Each component on the dashboard shows the total number of events, per device type, evaluated by a particular use case within the last hour.

If a component does not display any events, make sure the use case is configured properly. For example, the empty Events Monitored by Zero Day Attack Use Case component shown in the dashboard above might indicate that assets are not categorized as Internal Non Public-Facing, as required by that particular use case.

For more information about why a dashboard does not display events, see "Troubleshooting" on page 65.

3. Double-click one of the charts to see the events that originated from that device.

4. Return to the use case tab and open the RepSM Resource Health dashboard to review diagnostic information, such as messages from the Model Import Connector for RepSM Plus, rule error logs, and trend query failures.

   This dashboard also displays messages about RepSM Plus service activation and data retrieval. For an explanation of those messages, see "RepSM Plus Activation Messages" on page 1.

5. Return to the use case tab and open the RepSM Rules Health dashboard to make sure there are no disabled or deleted rules.

   ArcSight automatically disables rules that trigger too often. If this occurs, investigate the cause, as it might indicate an incorrect entry in the reputation data, or an incorrectly configured event source.

6. Return to the use case tab and open the RepSM Trend Health dashboard to check the status of trend queries.

A status of Failed might indicate that the query executed for too long and was stopped by ArcSight, or that a tablespace had insufficient free space.

Key Resources

The following table lists the key resources in this use case that might require configuration or that you might use during your investigation.

Monitor Resources that Support the RepSM Package Health Status Use Case

Resource	Description	Type	URI
Events Analyzed by RepSM Use Cases	This dashboard provides an overview of the traffic monitored for reputation data.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/
RepSM Rules Health	This dashboard provides an overview of rules in the RepSM package, including their status and logs.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/
RepSM Trend Health	This dashboard displays the Last 10 Trend Query Failures, Last 10 Trend Queries Returning No Results, and Trend Query Duration data monitors.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/
RepSM Resource Health	This dashboard shows an overview of the rule and trend functionality, as well as important connector events. For the RepSM Plus solution to function properly it is important that all trends and rules are enabled and that the Model Import Connector regularly updates the malicious entries lists. You can drill down from this dashboard to more specific rule and trend dashboards.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/

Monitor Resources that Support the RepSM Package Health Status Use Case, continued

Resource	Description	Type	URI
Latest Alert of RepSM MIC Health	The Reputation Security Monitoring Plus package monitors malicious or suspicious traffic based on reputation databases.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status
Error in RepSM Plus MIC Service Message	This rule is triggered when the RepSM mic cannot receive or process a malicious list.	Rule	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Monitor RepSM MIC Health/

Reputation Data Analysis

The Reputation Data Analysis use case provides statistical information about the entries in the reputation data. It also indicates when the data was last updated.

No special configuration is required for this use case.

To use the Reputation Data Analysis use case:

This section highlights some key features of the use case.

1. Click the **Use Cases** tab in the Navigator panel and open the **Reputation Data Analysis** use case located in:

   `/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus`

2. Open the Reputation Data Overview dashboard to see when the reputation data was last updated by the Model Import Connector for RepSM Plus.
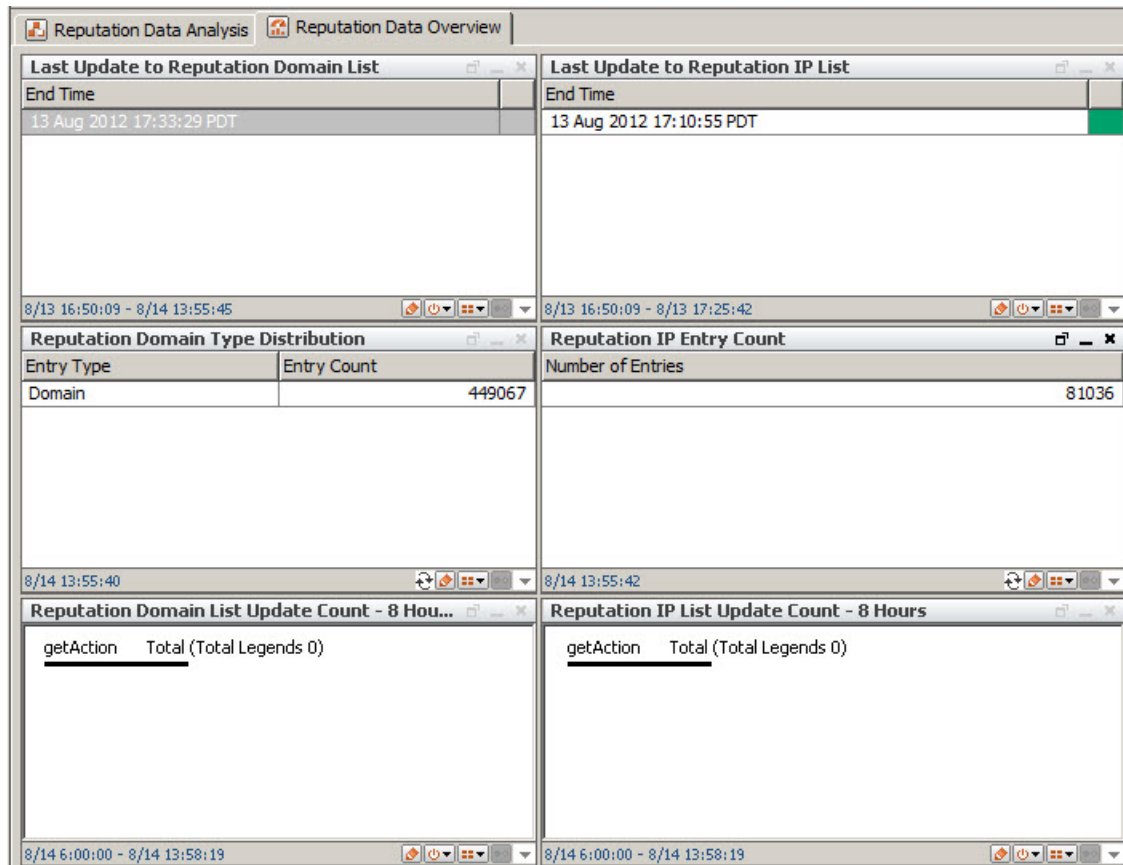
If the data has not been updated within the last 24 hours, there might be a problem with the connector.

You can review messages from the connector and determine its status by opening the RepSM Resource Health dashboard in the RepSM Package Health Status use case.

3. Return to the use case tab and open the Reputation Domain Database Overview dashboard to see the distribution of domains by exploit type and reputation score.

4. Double-click either the pie chart or histogram to display a list of the malicious domains by exploit type or reputation score.

    The Reputation IP Database Overview dashboard provides similar information for IP addresses.

5. Return to the use case tab to review the reports available for the use case.

Key Resources

The following table lists the key resources in this use case that you might use during your investigation.

Monitor Resources that Support the Reputation Data Analysis Use Case

Resource	Description	Type	URI
Reputation Data Overview	This dashboard provides a single view of the information in the malicious IP addresses and domain lists. You can double click the "Number of Entries" line in the middle component to drill down to a more detailed view of the specific list.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation IP Database Overview	This dashboard shows an overview of the reputation IP database (stored in an active list) in the system.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Domain Database Overview	This dashboard shows an overview of the reputation domain database (stored in an active list) in the system.	Dashboard	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Domain Entries	This query viewer shows the top 1,500,000 domain entries in the reputation domain active list.	Query Viewer	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation IP Entries	This query viewer shows the top 1,500,000 IP entries in the reputation IP active list.	Query Viewer	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Database Changes During the Last 1 Year	This report shows the reputation domain and IP database changes during the last year.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/

Monitor Resources that Support the Reputation Data Analysis Use Case, continued

Resource	Description	Type	URI
Reputation Database Changes During the Last 1 Year - Exploit Type Specific	This report shows the changes of a specific reputation exploit type during the last year.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Database Changes During the Last 1 Week - Exploit Type Specific	This report shows the changes of a specific reputation exploit type during the last week.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Database Changes During the Last 1 Week	This report shows the reputation domain and IP database changes during the last week.	Report	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/

Appendix A: Troubleshooting

This appendix provides information to help you resolve problems that might occur while installing and using RepSM Plus.

Installation fails with active list error

The installation of the RepSM Plus content package fails with the following error:

```
Install Failed: ActiveList capacity cannot be greater than nnnnnn
```

nnnnnn will vary depending on whether you are installing RepSM Plus on ArcSight ESM or ArcSight Express.

Solution:

Increase the active list maximum capacity, as described in "Configuring Active List Capacity (Required)" on page 15.

RepSM Plus uses cases not working

The RepSM Plus use cases do not appear to be working; their dashboards and reports do not display any events or reputation data.

Solution, in the following order:

1. Make sure the Model Import Connector for RepSM Plus is running.
2. Make sure the Model Import Connector for RepSM Plus is not out of memory. Look for an `OutOfMemoryError` message in the `$ARCSIGHT_HOME\current\logs\agent.log`. If necessary, increase the Model Import Connector for RepSM Plus Java heap memory size to at least 2 GB, as described in the *Model Import Connector for RepSM Plus Configuration Guide*.
3. Make sure the Model Import User is configured in the ArcSight Manager, as described in the *Model Import Connector for RepSM Plus Configuration Guide*. Otherwise, the Manager cannot accept reputation data from the RepSM Plus service.
4. Make sure the ArcSight Manager is collecting events from the devices described in "Supported Devices" on page 14.

5. Make sure the RepSM Plus rules are deployed, as described in "Deploying Rules" on page 24.

6. Make sure the use case is configured properly. Several use cases require asset categorization or other configuration to capture events. For configuration details, see "Configuring RepSM Plus Content" on page 19 and "Using RepSM Plus Content" on page 30.

7. Make sure inbound events are being sent to ArcSight Manager. Check the Inbound Events active channel.

8. Make sure outbound events are being sent to ArcSight Manager. Check the Outbound Events active channel.

9. Make sure the event source connector and ArcSight Manager are synchronized. The Manager Receipt Time should be no more than a few seconds later than the event End Time. Use the Inbound Events or Outbound Events active channel to open an event in the Event Inspector and compare these times.

Imported entries into Manager very low

The number of reputation data entries imported into the ArcSight Manager seems very low.

There might also be reputation data archive files that have a file extension of `xml.bad` in `ARCSIGHT_HOME\archive\webservices`.

Solution:

Make sure the following Model Import Connector for RepSM Plus property is set in the `agent.properties` file located at `ARCSIGHT_HOME\current\user\agent`:

`buildmodeldelay=60000`(one minute expressed in milliseconds)

This property controls how frequently the archives are sent to the Manager. If it is set too low, the connector will send archives too frequently. For more information about this property, see the *Model Import Connector for RepSM Plus Configuration Guide.*

Dashboards do not show recent activity

The RepSM Plus use case dashboards do not show any recent activity; the data seems stale.

Solution:

Check the Reputation Data Overview dashboard in the Reputation Data Analysis use case to see when the reputation data active lists were last updated. If the active lists have not been updated in the last 12 hours or so, there might be a problem with either the RepSM Plus service or the Model Import Connector for RepSM Plus. For example, the service might have expired or the connector might need to be restarted.

To check the status of either component, open the RepSM Package Health Status use case and review the messages in the RepSM Resource Health dashboard. For an explanation of the service messages, see "RepSM Plus Activation Messages" on page 1.

If the messages do not reveal any obvious issues, search the connector log at `$ARCSIGHT_HOME\current\logs\agent.log` for network error messages, such as:

- connection timeout
- host cannot be reached

and address those network issues.

If there are no obvious network issues, look for an `OutOfMemoryError` message in the `$ARCSIGHT_HOME\current\logs\agent.log`. If necessary, increase the Model Import Connector for RepSM Java heap memory size to at least 2 GB, as described in the *Model Import Connector for RepSM Plus Configuration Guide*.

While less likely, the problem might be caused by a planned outage of the RepSM Plus service. Check the RepSM group on the Micro Focus Security Community website to see if there is a planned outage:

Micro Focus Security Community

If you cannot determine cause of the problem, contact Customer Support.

Reputation data includes non-malicious entries

The reputation data includes an entry for an IP address or domain name that is not malicious.

Solution:

Consider adding an entry to the Exceptions active lists, as described in "Including and Excluding Entries from Reputation Data" on page 20.

To remove an entry permanently from the reputation data, gather the following information and contact Customer Support:

- The IP address or domain name to be removed.
- Any relevant event details (depending on the source of the event), such as the request URL, source port, destination port, and matching signature.

Dashboards display numerical exploit types

On ArcSight ESM, some dashboards display numerical exploit types. Exploit types should be text, such as Botnet, Spam, Spyware, or P2P.

Solution:

Increase the ArcSight Manager Java heap memory size to at least 4 GB, as described in the *ArcSight ESM Installation Guide*, and restart the Manager. Note that the Manager in ESM 6.9.1c or later has a default Java heap memory size at 16 GB.

Appendix B: Reputation Security Monitor Plus Resource Reference

This appendix lists all the Reputation Security Monitor Plus resources by type.

Active Channels

The following table lists all the active channels.

Active Channels Resources

Resource	Description	URI
All Events To or From Infected Assets During the Last 2 Hours	This active channel shows all events to or from the infected machines in the last two hours.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
All Interactions with Malicious Entities Detected During the Last 2 Hours	This active channel shows all the occurrences of rules that triggered to detect internal infections in this use case in the last two hours.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Inbound Events	This active channel shows events that the RepSM package considers as inbound.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Malicious Communication Matches Recently	This active channel displays all malicious communication match events during the last 2 hours.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Outbound Events	This active channel shows events that the RepSM package considers as outbound.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Events of Malicious Active List Changes	This channel shows any events related to the malicious list, such as add, delete or update the active list.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/`
RepSM Plus events	This channel shows all repsm plus mic events, which include received data, process and import data to the active list. It also shows all events which name contains RepSM.	`/All Active Channels/ArcSight Solutions/Reputation Security Monitor Plus/`

Active Lists

The following table lists all the active lists.

Active Lists Resources

Resource	Description	URI
Additional Malicious Domains	This active list enables user to define reputation domain names.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/User Defined Reputation Data/
Additional Malicious IP Addresses	This active list enables user to define reputation IP addresses.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/User Defined Reputation Data/
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Dangerous Browsing Exploit Types	This active list contains all exploit types considered as dangerous browsing.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Exceptions - Domains	This active list enable the user to define entries which will NOT be considered bad.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/User Defined Reputation Data/
Exceptions - IPs	This active list enable the user to define entries which will NOT be considered bad.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/User Defined Reputation Data/
Infected Internal Assets	This list contains all internal assets that were found to be communicating with malicious hosts (whose exploit types are defined in the Critical Exploit Types list). These assets are considered to be infected and should be investigated carefully. By default, a case will be opened for each asset in this list. When the case is closed, the asset will be removed from this list.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/

Active Lists Resources, continued

Resource	Description	URI
Interactions with Dangerous Destinations and Dangerous Sites	This list contains all outbound communications from a non public-facing assets to a malicious host with non-critical exploit types (the critical types are defined in the Critical Exploit Types active list and handled by the Internal Infected Assets use case). Each malicious destination is further classified as dangerous browsing or just dangerous destination, depending on the exploit type. The lists of dangerous browsing exploit types are defined by the Dangerous Browsing Exploit Types active list.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Internal Assets for Reputation Monitoring	This active list stores the addresses of all local assets that need to be monitored for existence in the reputation database.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Domains Found in Reputation Data	This active list stores the local domain names that appear in the reputation domain database. Entries in this list should be investigated.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Domains for Reputation Monitoring	This active list contains the domain names to be monitored for existence in the reputation database. The domain names in this list should be just the top two or three levels, such as microfocus.com or microfocus.co.uk.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal IP Addresses Found in Reputation Data	This active list stores all local IP addresses that appear in the reputation IP database.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Active Lists Resources, continued

Resource	Description	URI
Internal Network Addresses for Reputation Monitoring	This active list stores all local public network addresses (only class A, B or C) to be monitored for existence in the reputation database. If your network does not use these classes (for example, it uses CIDR instead), you can use the smallest class that fully represents your network. For example, a network address of 192.168.1.1/26 can be represented by a class C network of 192.168.1.0, so you can put 192.168.0. in this list. Note that for each network address entry , a dot (.) character is required.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Malicious Domains	This active list stores up to 1,500,000 reputation domain names.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/`
Malicious Host Names Involved in Internal Infections	This active list stores all malicious host names involved in internal infection incidents. It is used internally to show all base events, and has a time-to-live of one day.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Malicious Host Names in Dangerous Destination Interactions and Dangerous Browsing	This active list stores all malicious host names involved in interactions with dangerous destinations and dangerous sites. It is used internally to show all base events, and has a time-to-live of seven days.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Malicious Host Names in Dangerous Sources Access and Zero Day Attacks	This active list stores all malicious host names involved in interactions with dangerous sources and zero day attacks. It is used internally to show all base events, and has a time-to-live of seven days.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Malicious IP Addresses	This active list stores up to 1,500,000 reputation IP addresses.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/`
Scenarios	This active list maintains a list of the scenarios presented by General Use Case Scenarios. The Scenario Name field is compared against the Device Custom String6 field of the event.	`/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`

Active Lists Resources, continued

Resource	Description	URI
Support RepSM Advanced Content	This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Support/
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant to zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, and Miscellaneous.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with a zero day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
Track RepSM MIC		/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/
Dangerous Browsing Exploit Types	This active list contains all exploit types considered as dangerous browsing.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Interactions with Dangerous Destinations and Dangerous Sites	This list contains all outbound communications from a non public-facingassets to a malicious host with non-critical exploit types (the criticaltypes are defined in the Critical Exploit Types active list and handled by the Internal Infected Assets use case). Each malicious destination is further classified as dangerous browsing or just dangerous destination, depending on the exploit type. The lists of dangerous browsing exploit types are defined by the Dangerous Browsing Exploit Types active list.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/

Active Lists Resources, continued

Resource	Description	URI
Malicious Host Names in Dangerous Destination Interactions and Dangerous Browsing	This active list stores all malicious host names involved in interactions with dangerous destinations and dangerous sites. It is used internally to show all base events, and has a time-to-live of seven days.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Malicious Host Names in Dangerous Sources Access and Zero Day Attacks	This active list stores all malicious host names involved in interactions with dangerous sources and zero day attacks. It is used internally to show all base events, and has a time-to-live of seven days.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with a zero day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	/All Active Lists/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/

Dashboards

The following table lists all the dashboards.

Dashboards Resources

Resource	Description	URI
Events Analyzed by RepSM Use Cases	This dashboard provides an overview of the traffic monitored for reputation data.	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/
Geographical View of Malicious Communications	This dashboard provides an overview of traffic to reputation hosts.	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Internal Assets and Domains Found in Reputation Data	This dashboard provides information around internal assets or domain names reported in the reputation database.	/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Dashboards Resources, continued

Resource	Description	URI
Overview of Dangerous Browsing	This dashboard shows an overview of all dangerous browsing activities and access to dangerous destinations. You can drilldown to get to more information about the related destinations and the base events.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Overview of Internal Infections	This dashboard provides an overview of internal infected assets, including hosts that are communicating with external malicious entities, and the trend of infections over time. You can drilldown from the summary query viewers to specific interactions or base events.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Overview of Malicious Communication	This dashboard shows an overview of all malicious inbound and outbound communication events.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Overview of Zero Day Attacks	This dashboard shows an overview of all zero day attacks. You can drilldown to more information about the related sources and targets and the base events.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
RepSM Overview	This dashboard provides an overview of traffic from reputation hosts in the last 24 hours (not real time).	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Overview/`
RepSM Resource Health	This dashboard shows an overview of the rule and trend functionality, as well as important connector events. For the RepSM solution to function properly it is important that all trends and rules are enabled and that the Model Import Connector regularly updates the malicious entries lists. You can drill down from this dashboard to more specific rule and trend dashboards.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Rules Health	This dashboard provides an overview of rules in the RepSM package, including their status and logs.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`

Dashboards Resources, continued

Resource	Description	URI
RepSM Trend Health	This dashboard displays the Last 10 Trend Query Failures, Last 10 Trend Queries Returning No Results, and Trend Query Duration data monitors.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Reputation Data Overview	This dashboard provides a single view of the information in the malicious IP addresses and domain lists. You can double click the "Number of Entries" line in the middle component to drill down to a more detailed view of the specific list.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation Domain Database Overview	This dashboard shows an overview of the reputation domain database (stored in an active list) in the system.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation IP Database Overview	This dashboard shows an overview of the reputation IP database (stored in an active list) in the system.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Latest Alert of RepSM MIC Health	This dashboard shows latest alerts of repsm mic health.	`/All Dashboards/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`

Data Monitors

The following table lists all the data monitors.

Data Monitors Resources

Resource	Description	URI
Access to Malicious Entities	This data monitor shows a geographical view of all (successful or failed) access to malicious hosts or IP addresses.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Attacks from Malicious Entities	This data monitor shows a geographical view of all successful and failed inbound communications from malicious hosts or IP addresses.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Events Analyzed by Access from Dangerous Sources	This data monitor shows the count of all inbound communications in the last hour from all assets. These events are monitored by the Access from Dangerous Sources use case.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Event Statistics/
Events Analyzed by Access to Dangerous Destinations and Dangerous Browsing	This data monitor shows the count of all URL requests and outbound communications in the last hour from assets not categorized as Public-Facing.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Event Statistics/
Events Analyzed by Internal Infected Assets	This data monitor shows the count of all URL requests and outbound communications monitored by the Internal Infected Assets use case.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Event Statistics/
Events Analyzed by Zero Day Attack	This data monitor shows the count of all inbound communications in the last hour from all assets categorized as internal and non public-facing in the last hour. These events are monitored by the Zero Day Attacks use case.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Event Statistics/
Internal Infected Assets	This data monitor shows the last 20 internal infections. Select an entry and then right-click to drilldown into the Overview of Internal Infections dashboard.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Overview/

Data Monitors Resources, continued

Resource	Description	URI
Last 10 RepSM Trend Queries Returning No Results	This data monitor shows the last 10 trend queries that returned no results.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Trend Health/
Last 10 RepSM Trend Query Failures	This data monitor shows the last 10 trend query failures.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Trend Health/
Last Update to Reputation Domain List	This data monitor shows the last time an entry was added, modified or removed from the Malicious Domains active list. It can be used to ensure that the Model Import Connector for RepSM is operating properly and periodically updating the active list.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Last Update to Reputation IP List	This data monitor shows the last time an entry was added, modified, or removed from the Malicious IP Addresses active list. It can be used to ensure that the Model Import Connector for RepSM is operating properly and periodically updating the list.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Messages from Model Import Connector for RepSM	This data monitor shows important messages from the Model Import Connector for RepSM. These messages can indicate the connector is working properly, or can help you troubleshoot any issues.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Event Statistics/
Most Recent Dangerous Browsing Activities	This data monitor shows the last 20 dangerous browsing activities from non public-facing internal assets.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Most Recent Zero Day Attacks	This data monitor shows the last 20 zero day attacks to non public-facing internal assets.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/

Data Monitors Resources, continued

Resource	Description	URI
Recent Dangerous Browsing Destinations	This data monitor shows the last 20 dangerous browsing destinations from non public-facing internal assets.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Overview/`
Recently Triggered Rules	This data monitor shows the 10 recent RepSM rule triggerings.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Rule Health/`
RepSM Rule Error Logs	This data monitor shows the internal audit events related to RepSM rules. These events are generated when the rules are enabled/disabled or removed.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Rule Health/`
RepSM Rule States	This data monitor shows the last state of the RepSM rules as either enabled, disabled or deleted.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Rule Health/`
RepSM Trend Query Duration	This data monitor shows the duration of the last 20 successful trend queries. This data monitor is used in the Trends Status Dashboard.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Trend Health/`
RepSM Trend Query Runs Status	This Last State data monitor shows the status of the last RepSM trend queries. When a trend query starts, the trend state will be set to Running. If the trend query is successful, the trend state changes to Successful. If an error occurs and the trend query fails, the trend state changes to Failed.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Trend Health/`
Reputation Domain List Update Count - 8 Hours	This data monitor shows the count of all updates, additions, or deletions to the reputation domain active list during the last eight hours.	`/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`

Data Monitors Resources, continued

Resource	Description	URI
Reputation IP List Update Count - 8 Hours	This data monitor shows the count of all updates, additions or deletions to the reputation IP address active list during the last 8 hours.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Top Firing Rules	This data monitor shows the reputation traffic monitoring rule with most triggerings.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/Rule Health/
Zero Day Attacks	This data monitor shows the last 20 zero day attacks. Right-click to drilldown into the Overview of Zero Day Attacks dashboard.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Latest Alerts of RepSM MIC Health	This data monitor shows latest alerts for repsm mic health.	/All Data Monitors/ArcSight Solutions/Reputation Security Monitor Plus/

Global Variables

The following table lists all the global variables.

Global Variables Resources

Resource	Description	URI
Access from Dangerous Sources Reputation Domain Score Threshold	This variable stores the score threshold for malicious domain names used in the Access from Dangerous Sources use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Access from Dangerous Sources Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Access from Dangerous Sources use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Access to Dangerous Destinations Reputation Domain Score Threshold	This variable stores the score threshold for reputation domain names used in the Access to Dangerous Destinations use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Access to Dangerous Destinations Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Access to Dangerous Destinations use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`

Global Variables Resources, continued

Resource	Description	URI
Dangerous Browsing Reputation Domain Score Threshold	This variable stores the score threshold for malicious domain names used in the Dangerous Browsing use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Dangerous Browsing Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Dangerous Browsing use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Destination Address Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) IP based on the reputation IP data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Destination Address Reputation Score	This variable returns the reputation score of a malicious target (or a destination) host name based on the reputation IP data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`

Global Variables Resources, continued

Resource	Description	URI
Destination Domain Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) host name based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Destination Domain Reputation Score	This variable returns the reputation score of a malicious target (or a destination) address based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Destination Reputation Domain	This variable returns the reputation domain related to a malicious target (or destination) host name based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Internal Infected Assets Reputation Domain Score Threshold	This variable stores the score threshold for reputation domain names used in the Internal Infected Assets use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`

Global Variables Resources, continued

Resource	Description	URI
Internal Infected Assets Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Internal Infected Assets use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
RepSM Product	This global variables returns Reputation Security Monitor for events with reputation information. Otherwise, it returns the original Device Product.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Request URL Domain Reputation Exploit Type	This variable returns the exploit type of a domain from a URL request based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Request URL Domain Reputation Score	This variable returns the score of a domain from a URL request based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`

Global Variables Resources, continued

Resource	Description	URI
Request URL Reputation Domain	This variable returns the reputation domain from a URL request based on the reputation domain data.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Address Reputation Exploit Type	This variable returns the exploit type of a malicious attacker (or a source) IP address based on the reputation IP data.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Address Reputation Score	This variable returns the reputation score of a malicious attacker (or a source) host name based on the reputation IP data.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/
Source Domain Reputation Exploit Type	This variable returns the exploit type of a malicious attacker (or a source) host name based on the reputation domain data.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/

Global Variables Resources, continued

Resource	Description	URI
Source Domain Reputation Score	This variable returns the reputation score of a malicious attacker (or a source) host name based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Source Reputation Domain	This variable returns the reputation domain (or host name) related to a malicious attacker (or source) host name based on the reputation domain data.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Event Enrichment with Reputation Data/`
Zero Day Attacks Reputation Domain Score Threshold	This variable stores the score threshold for malicious domain names used in the Zero Day Attacks use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
Zero Day Attacks Reputation IP Score Threshold	This variable stores the score threshold for reputation IP addresses used in the Zero Day Attacks use case.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/`
solnCheckDestinationIsInExceptionsDomainList	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/`

Global Variables Resources, continued

Resource	Description	URI
solnCheckSourceIsInExceptionsDomainList	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Configuration/
solnGetAttackerDomainExploitType	This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetAttackerDomainLevel1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetAttackerDomainLevel2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/

Global Variables Resources, continued

Resource	Description	URI
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetAttackerReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/

Global Variables Resources, continued

Resource	Description	URI
solnGetAttackerReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetAttackerReputationHostNameListEntry	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/`
solnGetBaseRequestURLAdditionalDataDomainEntry	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/`
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetBaseRequestURLDomainExceptoinEntry	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/`

Global Variables Resources, continued

Resource	Description	URI
solnGetDestinationAdditionalDataDomainEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetDestinationAdditionalDataDomainLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetDestinationAdditionalDataDomainLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetDestinationAdditionalDataDomainLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetDestinationAdditionalDataHostNameListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetDestinationAdditionalDataIPListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetDestinationDomain	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Destination/
solnGetDestinationExceptionDomainLevel1ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/

Global Variables Resources, continued

Resource	Description	URI
solnGetDestinationExceptionDomainLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetDestinationExceptionDomainLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetDestinationExceptionDomainLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetDestinationExceptionHostNameListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetDestinationExceptionIPListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetDestinationExceptions	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Destination/
solnGetDestinationExploitType	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Destination/
solnGetDestinationIP	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Destination/

Global Variables Resources, continued

Resource	Description	URI
solnGetDestinationScore	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Destination/
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetLowerDestinationHostName	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetLowerSourceHostName	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetLowerTargetHostName	This variable returns the target host name in lower case.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetRequestURLAdditionalDataDomainEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetRequestURLAdditionalDataDomainLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetRequestURLAdditionalDataDomainLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetRequestURLAdditionalDataDomainLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/

Global Variables Resources, continued

Resource	Description	URI
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetRequestURLDomainExceptionLevel1ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetRequestURLDomainExceptionLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetRequestURLDomainExceptionLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetRequestURLDomainExceptionLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/

Global Variables Resources, continued

Resource	Description	URI
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/`
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/`
solnGetRequestURLDomainLevel3ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`

Global Variables Resources, continued

Resource	Description	URI
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetRequestURLExceptoinDomainEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetRequestURLReputationDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetSourceAddirionalDataIPListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetSourceAdditionalDataDomainEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/

Global Variables Resources, continued

Resource	Description	URI
solnGetSourceAdditionalDataDomainLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetSourceAdditionalDataDomainLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetSourceAdditionalDataDomainLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetSourceAdditionalDataHostNameListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Additional User Data/
solnGetSourceDomain	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Source/
solnGetSourceExceptionDomainLevel1ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetSourceExceptionDomainLevel2ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
solnGetSourceExceptionDomainLevel3ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/

Global Variables Resources, continued

Resource	Description	URI
soInGetSourceExceptionDomainLevel4ListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
soInGetSourceExceptionHostNameListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/Check Exceptions/
soInGetSourceExceptionIPListEntry	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
soInGetSourceExceptions	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Source/
soInGetSourceExploitType	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Source/
soInGetSourceIP	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Source/
soInGetSourceScore	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By Source/

Global Variables Resources, continued

Resource	Description	URI
solnGetTargetDomainExploitType	This variable returns the exploit type of a target in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetTargetDomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetTargetDomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/
solnGetTargetDomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/

Global Variables Resources, continued

Resource	Description	URI
solnGetTargetReputationDomainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetTargetReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/

Global Variables Resources, continued

Resource	Description	URI
solnGetTargetReputationHostNameListEntry	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/`
solnGetTargetReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/`
solnGetURLDomain	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By URL Request/`
solnGetURLExceptions	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By URL Request/`
solnGetURLExploitType	This resource has no description.	`/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By URL Request/`

Global Variables Resources, continued

Resource	Description	URI
solnGetURLIP	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By URL Request/
solnGetURLScore	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Main Final Variables/Entry By URL Request/
solnNullAddress	This resource has no description.	/All Fields/ArcSight Solutions/Reputation Security Monitor Plus/Support/

Field Sets

The following table lists all the field sets.

Field Sets Resources

Resource	Description	URI
Events with Source Reputation Information	This field set contains fields with source reputation domain or IP address information.	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Events with Target Reputation Information	This field set contains fields with target reputation domain or IP address information.	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Internal Infections	This field set provides the fields relevant to the correlation events generated by the detection rules in this use case.	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Reputation Domain Enrichment	This field set contains fields with reputation domain information for event enrichment purposes.	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/
Reputation IP Enrichment	This field set contains fields with reputation IP information for event enrichment purposes.	/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/

Field Sets Resources, continued

Resource	Description	URI
Request URL Enrichment	This field set contains fields with reputation information (based on the request URL) for event enrichment purposes.	`/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/`
System Events	This resource has no description.	`/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/`
Active List Events	This field set selects fields related to the active list events.	`/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/`
RepSM MIC Events	This field set contains fields with RepSM MIC events.	`/All Field Sets/ArcSight Solutions/Reputation Security Monitor Plus/`

Filters

The following table lists all the filters.

Filters Resources

Resource	Description	URI
Zero Day Attack Reputation Domain Exploit Types	This filter identifies events from malicious domain names or host names with zero-day attack exploit types.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/Support/`
Access from Dangerous Sources	This filter identifies all access from dangerous sources. By default, any successful inbound communication not flagged as a zero day attack is flagged as such.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Access from Dangerous Sources - Rule Firings	This filter identifies all correlation events generated by rules that detect access from dangerous sources.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Access to Dangerous Destinations	This filter identifies all access to dangerous destinations.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`

Filters Resources, continued

Resource	Description	URI
Attacker Host Name Present	This filter checks whether the Attacker Host Name field is populated.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/Support/
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/Support/
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/Support/
Dangerous Browsing	This filter identifies all dangerous browsing activities.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities - Rule Firings	This filter identifies all firings of rules that detect dangerous browsing activities.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/Support/
Dangerous Browsing Target Reputation Domain Exploit Types	This filter identifies events to target reputation domain or host name considered as of dangerous browsing exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/Support/
Dangerous Browsing Target Reputation IP Exploit Types	This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/Support/

Filters Resources, continued

Resource	Description	URI
Dangerous Communication	This filter detects Layer 1 events.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Dangerous Destinations and Dangerous Browsing: Outbound Communication to Malicious Domains	This filter identifies all outbound communication non public-facing assets to malicious entities with non critical exploit types and high scores.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Dangerous Destinations and Dangerous Browsing: Outbound Communication to Malicious IPs	This filter identifies all outbound communication from non public-facing assets to any reputation IP with non critical exploit type and high score.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Dangerous Destinations and Dangerous Browsing: Outbound URL Requests to Malicious Domains	This filter identifies all outbound URL requests from non public-facing assets to any reputation domain with non critical exploit type and high score.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Dangerous Inbound Communication	This filter detects malicious inbound events.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Dangerous Outbound Communication	This filter detects malicious outbound events.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Event Limit	This filter limits the events processed and reported by the solution to only the events that are relevant to the regulation. This filter is included in the conditions of all other resources in the package, such as rules, queries, and filters, either directly or indirectly. Edit this filter to change the events processed and reported by this solution.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Events Monitored by Access from Dangerous Sources Use Case	This filter identifies all events monitored by the Access from Dangerous Sources use case. These events reflect inbound communications to all assets.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/

Filters Resources, continued

Resource	Description	URI
Events Monitored by Access to Dangerous Destinations and Dangerous Browsing Use Cases	This filter identifies all events monitored by Access to Dangerous Destinations and Dangerous Browsing use cases. These events contain request URLs, or reflect outbound communication from assets not categorized as Public-Facing.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Events Monitored by Internal Infected Assets Use Case	This filter identifies all events monitored by the Internal Infected Assets use case. These events contain request URLs, or reflect outbound communication.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Events Monitored by Zero Day Attack Use Case	This filter identifies all events monitored by the Zero Day Attacks use case. These events reflect inbound communications to assets categorized as internal, non public-facing.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Events from Internal Infected Assets	Filter events for pattern discovery Internal Infected Assets	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Events from Malicious Sources	This filter identifies events whose attackers are found in the reputation database.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/`
Events from Model Import Connector for RepSM	This filter identifies important events generated by the RepSM Model Import Connector.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Events to Malicious Targets	This filter identifies events whose targets are found in the reputation database.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/`
Events with Requests to Malicious Hosts	This filter identifies events with requests to hosts found in the reputation database.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/`

Filters Resources, continued

Resource	Description	URI
Inbound Communication from Malicious Domains	This filter identifies all inbound traffic from domain names in the reputation domain active list.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/Malicious Communications/
Inbound Communication from Malicious IP Addresses	This filter identifies all inbound traffic from IP addresses in the reputation IP active list for real time correlation.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/Malicious Communications/
Inbound Events	This filter identifies events coming from outside your network, targeting your organization.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Infected Assets: Outbound Communication to Malicious Domains	This filter identifies all outbound traffic either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Infected Assets: Outbound Communication to Malicious IPs	This filter identifies all outbound traffic either from internal assets to reputation IP addresses with high scores and critical exploit types, or from public-facing assets to any reputation IP.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Infected Assets: Outbound URL Requests to Malicious Domains	This filter identifies all outbound URL requests either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Interactions with Dangerous Destinations - Rule Firings	This filter identifies all firings of rules that detect interactions with dangerous destinations (i.e. non-browsing exploit types).	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/

Filters Resources, continued

Resource	Description	URI
Internal Infected Asset Case Creation or Removal	This filter identifies events generated when the active list storing internal infection records is modified.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Internal Traffic	This filter identifies traffic within the network of your organization.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Non Public-Facing Internal Targets	This filter identifies all events for which the targets are categorized as non public-facing internal.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Outbound Communication to Reputation Domains	This filter identifies all outbound traffic to domain names in the reputation domain active list used for real time correlation.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/Malicious Communications/
Outbound Communication to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/Malicious Communications/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Peer To Peer	This filter detects the peer-to-peer scenario.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Potential Spear Phishing	This filter detects the spam scenario.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/

Filters Resources, continued

Resource	Description	URI
Public-Facing Targets	This filter identifies all events whose targets are categorized as public-facing, for example, web servers.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/`
RepSM Relevant Events	This filter identifies events that contains information related to reputation data (for example, host address or request URL).	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Events Enrichment with Reputation Data/`
RepSM Rule Firing Events	This filter identifies all triggerings of RepSM rules.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Rules Engine Events	This filter identifies all internal audit events related to RepSM rules.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Trend Query Duration	This filter identifies successful RepSM trend query run events.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Trend Query Failure	This filter identifies failed RepSM trend query run events.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Trend Query Returning No Results	This filter identifies successful RepSM trend query run events, where the number of rows inserted in the trend is 0.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
RepSM Trend Runs Status	This filter identifies trend query run events.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM Package Health Status/`
Reputation Domain Changes	This filter identifies events that indicate a change was made to the reputation domain active list.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`

Filters Resources, continued

Resource	Description	URI
Reputation IP Changes	This filter identifies events that indicate a change was made to the reputation IP address active list.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation Inbound Communication	This filter identifies all events from a malicious host or IP address.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Reputation Outbound Communication	This filter identifies all communication to a malicious host or IP address.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
Request to Reputation Domains	This filter identifies all URL requests to domain names in the reputation domain active list used for real time correlation.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/Malicious Communications/
Scenarios Events	This filter detects Layer 2 events (scenario events); the scenarios found in the Scenarios active list.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Success Events from Internal Infected Assets	Filter events for pattern discovery "Potential Intrusion Investigation".	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/General/
Traffic to or from Hosts with Host Names	This filter identifies all traffic to or from hosts with host name information.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Traffic to or from Internal IP Address in Reputation Data	This filter identifies all traffic to IP addresses found in reputation data.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Zero Day Attack List Manipulation	This filter identifies events generated when the active list storing zero day attack records is modified.	/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Overview/

Filters Resources, continued

Resource	Description	URI
Zero Day Attack Reputation IP Exploit Types	This filter identifies events from malicious IP addresses with zero day attack exploit types.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/Support/`
Zero Day Attacks	This filter identifies all potential zero day attacks. By default, any successful inbound communication from a malicious domain or host name, or IP address with a zero-day attack exploit type is flagged as such.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks - Rule Firings	This filter identifies all correlation events generated by rules that detect zero day attacks.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
RepSM MIC Health Alerts	This filter selects alerts which URL is under RepSM MIC.	`/All Filters/ArcSight Solutions/Reputation Security Monitor Plus/RepSM MIC Health Alerts`

Integration Commands

The following table lists all the integration commands.

Integration Commands Resources

Resource	Description	URI
Search Selected Item in Google	This command performs a Google search of the selected cell. It can be used to investigate the reputation entity.	`/All Integration Commands/ArcSight Solutions/Reputation Security Monitor Plus/`

Integration Configurations

The following table lists all the integration configurations.

Integration Configurations Resources

Resource	Description	URI
Search Selected Item in Google	This configuration is used for the Search Selected Item in Google command. It can be used in any viewer or editor.	`/All Integration Configurations/ArcSight Solutions/Reputation Security Monitor Plus/`

Packages

The following table lists all the packages.

Package Resources

Resource	Description	URI
Reputation Security Monitor Plus 1.8	Reputation Security Monitoring Plus package monitors malicious or suspicious traffic based on reputation database.	`/All Packages/ArcSight Solutions/Reputation Security Monitor Plus 1.8`

Profiles

The following table lists all the profiles.

Profiles Resources

Resource	Description	URI
Behavior of Internal Infected Assets	This profile enables pattern discovery to analyze behavior of internal infected assets.	`/All Profiles/ArcSight Solutions/Reputation Security Monitor Plus/`
Complex Attacks Investigation	This profile enables pattern discovery to detect and understand complex malicious activities.	`/All Profiles/ArcSight Solutions/Reputation Security Monitor Plus/`
Potential Intrusion Investigation	This profile looks for successful inbound communication patterns of assets which successfully received communication from malicious hosts.	`/All Profiles/ArcSight Solutions/Reputation Security Monitor Plus/`
Zero Day Investigation	This profile discovers patterns of communication attempts from the same malicious address to different internal assets.	`/All Profiles/ArcSight Solutions/Reputation Security Monitor Plus/`

Queries

The following table lists all the queries.

Queries Resources

Resource	Description	URI
Reputation IP Score Histogram	This query builds the histogram of the reputation IP score.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Access from Dangerous Sources in the Last 24 Hours	This query returns all access from dangerous sources in the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Access from Dangerous Sources per Reputation Type During the Last 24 Hours	This query returns the count of access from dangerous sources per reputation exploit type during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Access to Dangerous Destinations by Types During the Last 7 Days	This query returns the total count of access to dangerous destinations (domain, host name, or IP address) during the last seven days. It is based on a trend so it might not show most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Overview/`
All Access to Dangerous Destinations Currently Stored	This query returns the access to dangerous destinations by internal hosts currently stored in a list.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
All Base Events During the Last 24 Hours for Dangerous Destinations and Browsing - Drilldown Only	This query returns all events during the last 24 hours and should only be used as a drilldown.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
All Base Events During the Last 24 Hours for Zero Day Attacks and Access from Dangerous Sources - Drilldown Only	This query returns all events during the last 24 hours and should only be used as a drilldown.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`

Queries Resources, continued

Resource	Description	URI
All Base Events to or from Infected Assets During the Last 24 Hours	This query returns all events related to internal infected assets during the last 24 hours and should only be used as a drilldown.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
All Browsing Activities Currently Stored	This query returns the dangerous browsing activities by internal hosts currently stored in a list.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
All Correlation Events on Dangerous Browsing and Access to Dangerous Destinations	This query returns all correlations events generated by the rules that detect dangerous browsing and access to dangerous destinations.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
All Correlation Events on Zero Day Attacks and Access from Dangerous Sources	This query returns all correlations events generated by the rules that detect zero day attacks and access from dangerous sources.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
All Events to or from Infected IP Addresses During the Last 24 Hours	This query returns all events related to internal infected IP addresses during the last 24 hours. It relies on the infected IP addresses stored in an active list.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
All Events to or from Internal Hosts Found in Reputataion Data	This query returns all events related to host names that belong to an internal domain found in reputation data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
All Events to or from Internal IP Addresses Found in Reputation Data within the Last 24 Hours	This query returns all events related to IP addresses found in reputation data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
All Events with Host Name Information within the Last 24 Hours - Drilldown Only	This query returns all events with host name information during the last 24 hours and should be used for drilldown purposes only.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`

Queries Resources, continued

Resource	Description	URI
All Inbound and Outbound Communication related to Infected Assets During the Last 24 Hours	This query returns all inbound and outbound traffic to or from an infected asset during the last 24 hours. This query does not look at internal traffic.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Infection Base Events During the Last 24 Hours	This query returns all events during the last 24 hours and should only be used as a drilldown.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Interactions with Malicious Entities Detected During the Last 24 Hours	This query returns all incidents of internal infections based on the detection rule firings in the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Internal Communication to or from Infected Assets During the Last 24 Hours	This query returns all internal traffic to or from an infected asset during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Internal Domains Found	This query returns all local domains that appear in the reputation domain database.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
All Internal IP Addresses Found	This query returns all local IPs that appear in the reputation domain database.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
All Occurrences of Access from Dangerous Sources Currently Stored	This query returns the occurrences of access from dangerous sources to internal hosts currently stored in an active list.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
All System Events on The Last day	This query retrieves all the non-ArcSight internal events during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

Queries Resources, continued

Resource	Description	URI
All Zero Day Attacks Currently Stored	This query returns the zero day attacks to internal hosts currently stored in an active list.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Assets Infected for More Than A Week	This query returns all infected internal assets that have remained in the infected list over one week. This usually means the related cases have not been or are still being investigated.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Address Infection Drilldown Only	This query returns outbound events in which the target address appears on the malicious list during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Hostname Infection Drilldown Only	This query returns outbound events in which the target host name appears on the malicious list during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Request Infection Drilldown Only	This query returns outbound events in which the request URL appears on the malicious list during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Communications from Internal Assets to Dangerous Destinations	This query returns all communication from internal machines to dangerous destinations.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Communications from Internal Assets to Dangerous Sites	This query returns all communication from internal machines to dangerous destinations, considered to be dangerous browsing.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Currently Infected Assets and Recorded Interactions with Malicious Entities	This query returns all internal infected assets detected through communications with reputation IPs or domains.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/

Queries Resources, continued

Resource	Description	URI
Daily Communications with Dangerous Destinations During the Last 7 Days	This query returns the top daily count of communications with dangerous destinations (domain, host name or IP address) during the last seven days. It is based on a trend so it might not show most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Daily Count of Access from Dangerous Sources During the Last 7 Days	This query returns the daily count of access from dangerous sources during the last seven days. It is based on a trend so it might not show most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Daily Count of Zero Day Attacks During the Last 7 Days	This query returns the daily count of zero day attacks during the last seven days. It is based on a trend so it might not show most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Daily Dangerous Browsing Activities During the Last 7 Days	This query returns the top daily count of dangerous activities during the last seven days. It is based on a trend so it might not show most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing Activities During the Last 7 Days	This query returns dangerous browsing activities during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing Activities in the Last 24 Hours	This query returns all dangerous browsing activities in the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing Activities per Reputation Type During the Last 24 Hours	This query returns the number of dangerous browsing activities per reputation exploit type during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing Activities per Reputation Type During the Last 30 Days	This query returns the number of dangerous browsing activities per reputation exploit type during the last 30 days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`

Queries Resources, continued

Resource	Description	URI
Dangerous Browsing Activities per Reputation Type During the Last 7 Days	This query returns the number of dangerous browsing activities per reputation exploit type during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing Activities per Reputation Type During the Last One Year	This query returns the number of dangerous browsing activities per reputation exploit type during the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Dangerous Browsing and Interactions with Dangerous Destinations - Trend Base	This query returns all firings of rules that detect dangerous browsing or access to dangerous destinations during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Dangerous Destinations Accessed by Internal Assets	This query returns the summary of dangerous destinations contacted by internal hosts.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Dangerous Websites Accessed by Internal Assets	This query returns the summary of dangerous web sites contacted by internal hosts.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Distribution of Dangerous Destination Exploit Types	This query returns the distribution of dangerous destinations contacted by internal hosts.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Distribution of Dangerous Destination Types	This query returns the distribution of dangerous destinations and dangerous browsing activities.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Events per Scenarios During the Last Day - On Trend	This query retrieves all the scenario events during the last day, grouped by scenario type.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`

Queries Resources, continued

Resource	Description	URI
Hourly Count of Inbound Events on the Last Day -On Trend	This query is the base query for communication from malicious sources during the last day.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Hourly Count of Outbound Events on the Last Day -On Trend	This query is the base query for communication to malicious destinations during the last day.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Infected Asset List Snapshot - Trend Base	This query returns a snapshot of internal infected assets. It is used by a daily trend for long term data analysis.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Infection Types over Last Month	This query returns the weekly count of internal infected assets over the last month.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Interactions with Dangerous Destinations in the Last 24 Hours	This query returns all interactions with dangerous destinations (non-browsing types only) in the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Interactions with Dangerous Destinations per Reputation Type During the Last 24 Hours	This query returns the number of interactions to dangerous destinations (non-browsing types) per reputation exploit type during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Internal Asset Reputation Detector (Asset Based) - Trend Base	This query returns the list of internal assets that appear in the reputation IP database.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
Internal Asset Reputation Detector (List Based) - Trend Base	This query returns all internal hosts that appear in the reputation IP database. It runs on top of the reputation IP database and correlates with the assets to be monitored, as defined in an active list.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Queries Resources, continued

Resource	Description	URI
Internal Assets Communicated with Dangerous Destinations	This query returns the summary of internal assets that communicated with a dangerous destination.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Internal Assets Involved in Dangerous Browsing	This query returns the summary of internal assets involved in dangerous browsing.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Internal Assets with Bad communication - On Trend	This query retrieves a list of all internal assets involved in bad communication. It is used as a base query for a report.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Internal Domain Reputation Detector (List Based) - Trend Base	This query returns all internal domain names that appear in the reputation domain database. It runs on top of the reputation domain database and correlates with the specified domain names.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Internal Infected Asset Count per Month	This query returns the count of internal infected assets detected per month over the last year.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Internal Infected Asset Count per Week	This query returns the weekly count of internal infected assets detected during the last month.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Internal Infected Assets - Long Term	This query returns a list of internal infected assets during the last year.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Layer 1 Events - Trend Base	This query retrieves all of the layer 1 events during the last hour, and is used by a trend.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`

Queries Resources, continued

Resource	Description	URI
Layer 2 Events - Trend Base	This query retrieves all of the Layer 2 events during the last hour, and is used by a trend.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
List of Layer 1 events on the Last 7 days On Trend	This query runs over the Layer 1 trend for the last seven days.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
List of Malicious Inbound Events -On Trend	This query retrieves all of the malicious inbound events for the last seven days.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
List of Malicious Outbound Events -On Trend	This query retrieves all of the malicious outbound events during the last seven days.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Monthly Count of Dangerous Browsing Activities During the Last One Year	This query returns the number of dangerous browsing activities per month during the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Monthly Count of Dangerous Browsing Activities per Source Zone During the Last One Year	This query returns the weekly count of dangerous browsing activities per source zone during the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Monthly Count of Dangerous Browsing Activities per Type During the Last One Year	This query returns the monthly count of dangerous browsing activities per exploit type during the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Monthly Count of Zero Day Attacks During the Last One Year	This query returns the number of zero day attacks per month within the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`

Queries Resources, continued

Resource	Description	URI
Monthly Count of Zero Day Attacks per Target Zone During the Last One Year	This query returns the weekly count of zero day attacks per source zone within the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Monthly Count of Zero Day Attacks per Type During the Last One Year	This query returns the monthly count of zero day attacks per exploit type during the last year. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Reputation Domain Changes During the Last 1 Week	This query returns the count of reputation domain entries during the last week.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Changes During the Last 1 Week - Exploit Type Specific	This query returns the count of a specific reputation domain exploit type during the last week.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Changes During the Last 1 Year	This query returns the monthly average count of reputation domain entries during the last year.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Changes During the Last 1 Year - Exploit Type Specific	This query returns the count of a specific reputation domain exploit type during the last year.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Changes by Type During the Last 1 Week	This query returns the count of reputation domain exploit types during the last week.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Count - Trend Base	This query returns the count of reputation domains, grouped by the exploit type and domain type.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`
Reputation Domain Entries	This query returns the top 1,500,000 domain entries in the reputation domain active list.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/`

Queries Resources, continued

Resource	Description	URI
Reputation Domain Entry Count by Type	This query returns the current count of reputation domains and host names.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation Domain Score Histogram	This query builds the histogram of the reputation domain score.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation Domain by Exploit Type	This query returns the reputation domain count per exploit type.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Changes - Trend Base	This query returns the count of reputation addresses, grouped by the exploit type.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Changes During the Last 1 Week	This query returns the count of reputation addresses during the last week.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Count During the Last 1 Week - Exploit Type Specific	This query returns the count of reputation IP exploit types during the last week.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Count During the Last 1 Year - Exploit Type Specific	This query returns the count of reputation IP exploit types during the last year.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Count by Type During the Last 1 Week	This query returns the count of reputation IP exploit types during the last week.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Count by Type During the Last 1 Year	This query returns the monthly average count of reputation IP exploit types over the last year.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/

Queries Resources, continued

Resource	Description	URI
Reputation IP Entries	This query returns the top 1,500,000 IP entries in the reputation IP active list.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP Entry Count	This query returns the current number of reputation addresses.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Reputation IP by Exploit Type	This query returns the count of reputation addresses per exploit type.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Database Analysis/
Scenario Events During the Last 7 Days-On Trend	This query retrieves all of the scenario events for the last seven days.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Status Distribution of Open Case on Zero Day Attacks	This query returns all open cases on zero day attacks, grouped by case status.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Status Distribution of Open Cases on Internal Infected Assets	This query returns a list of all open cases for internal infected assets, grouped by case status.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Summary of Contacted Malicious Hosts	This query returns the summary of malicious hosts contacted by infected internal hosts.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Summary of Currently Infected Assets	This query returns the summary of internal infected machines detected through communications with reputation IP addresses or domains.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/

Queries Resources, continued

Resource	Description	URI
Summary of Dangerous Sources	This query returns the dangerous sources accessing internal, non-public facing assets, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Summary of Internal Assets Accessed by Dangerous Sources	This query returns the summary of internal assets accessed by dangerous sources, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected and the time of the latest attack.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Summary of Internal Assets Targeted by Zero Day Attacks	This query returns the summary of internal assets targeted by zero day attacks, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected and the time of the latest attack.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Summary of Open Cases on Internal Infected Assets	This query returns all open cases for internal infected assets.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Summary of Open Cases on Zero Day Attacks	This query returns all open cases on zero day attacks.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Summary of Zero Day Attackers	This query returns the sources of zero day attacks, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Top 10 Dangerous Browsing Destinations Accessed by Most Internal Assets During the Last 24 Hours	This query returns the top dangerous browsing destinations (domain, host name or IP address) that have the highest number of internal assets interacted with during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Top 10 Dangerous Browsing Destinations Accessed by Most Internal Assets During the Last 7 Days	This query returns the top dangerous browsing destinations (domain, host name or IP address) that have the highest number of internal assets accessed during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`

Queries Resources, continued

Resource	Description	URI
Top 10 Dangerous Browsing Destinations Most Accessed During the Last 24 Hours	This query returns the top dangerous browsing destinations (domain, host name or IP address) that were accessed the most during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Top 10 Dangerous Browsing Destinations Most Accessed During the Last 7 Days	This query returns the top dangerous browsing destinations (domain, host name or IP address) that were accessed the most during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Top 10 Dangerous Destinations Accessed by Most Internal Assets During the Last 24 Hours	This query returns the top dangerous destinations (domain, host name or IP address) of non-browsing types that have the highest number of internal assets interacted with during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Top 10 Dangerous Destinations Most Accessed During the Last 24 Hours	This query returns the top dangerous destinations (domain, host name or IP address) of non-browsing exploit types that were accessed the most during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Top 10 Zero Day Attackers Attacked Most Internal Hosts During the Last 7 Days	This query returns the zero day attackers that attacked the highest number of internal hosts during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Top 10 Zero Day Attackers During the Last 7 Days	This query returns the top zero day attackers, based on event count, during the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Top 20 Internal Assets with Bad communication -On Trend	This query retrieves the top 20 internal assets with bad communication. It is used as a base query for a query viewer.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Top Accessed Assets During the Last 24 Hours	This query returns the internal assets being accessed the most during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`

Queries Resources, continued

Resource	Description	URI
Top Assets Interacted Most with Dangerous Destinations During the Last 24 Hours	This query returns the internal assets that interacted most with dangerous destinations (non-browsing exploit types) during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Top Assets Most Attacked During the Last 7 Days	This query returns the internal assets targeted most by zero day attacks during the last seven days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Top Assets with Most Dangerous Browsing Activities During the Last 24 Hours	This query returns the internal assets that interacted most with dangerous destinations that have non-browsing exploit types during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Top Assets with Most Dangerous Browsing Activities During the Last 7 Days	This query returns the internal assets with most browsing activities during the last seven days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Top Attacked Assets During the Last 24 Hours	This query returns the internal assets attacked most during the last 24 hours.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Weekly Count of Dangerous Browsing Activities During the Last 30 Days	This query returns the number of dangerous browsing activities per week during the last 30 days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Weekly Count of Dangerous Browsing Activities per Source Zone During the Last 30 Days	This query returns the weekly count of dangerous browsing activities per source zone during the last 30 days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Weekly Count of Dangerous Browsing Activities per Type During the Last 30 Days	This query returns the weekly count of dangerous browsing activities per exploit type during the last 30 days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/

Queries Resources, continued

Resource	Description	URI
Weekly Count of Zero Day Attacks During the Last 30 Days	This query returns the number of zero day attacks per week within the last 30 days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Weekly Count of Zero Day Attacks per Target Zone During the Last 30 Days	This query returns the weekly count of zero day attacks per target zone within the last 30 days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Weekly Count of Zero Day Attacks per Type During the Last 30 Days	This query returns the weekly count of zero day attacks per exploit type within the last 30 days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attack Details During the Last 7 Days	This query returns the details of zero day attacks within the last seven days. This query is based on a trend so it might not show the most recent data.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks and Access from Dangerous Sources - Trend Base	This query returns all firings of rules that detect zero day attacks or access from dangerous sources during the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks in the Last 24 Hours	This query returns all zero day attacks in the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks per Reputation Type During the Last 24 Hours	This query returns the number of zero day attacks per reputation exploit type within the last 24 hours.	`/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`

Queries Resources, continued

Resource	Description	URI
Zero Day Attacks per Reputation Type During the Last 30 Days	This query returns the number of zero day attacks per reputation exploit type within the last 30 days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks per Reputation Type During the Last 7 Days	This query returns the number of zero day attacks per reputation exploit type within the last seven days. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks per Reputation Type During the Last One Year	This query returns the number of zero day attacks per reputation exploit type within the last year. This query is based on a trend so it might not show the most recent data.	/All Queries/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/

Query Viewers

The following table lists all the query viewers.

Query Viewers Resources

Resource	Description	URI
Access to Dangerous Destinations by Exploit Types	This query viewer shows the total count of access to dangerous destinations (domain, host name or IP address) during the last seven days. It is based on a trend so it might not show most recent data.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Overview/
All Access to Dangerous Destinations Currently Stored	This query viewer shows the access to dangerous destinations by internal hosts currently stored in a list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
All Base Events During the Last 24 Hours for Zero Day Attacks and Access from Dangerous Sources - Drilldown Only	This query viewer shows all events during the last 24 hours and should only be used as a drilldown.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/

Query Viewers Resources, continued

Resource	Description	URI
All Base Events for Dangerous Destinations and Browsing - Drilldown Only	This query viewer shows all events during the last 24 hours and should only be used for drilldown during this use case.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
All Base Events to or from Infected Assets During the Last 24 Hours	This query viewer shows all events related to internal infected assets during the last 24 hours and should only be used as a drilldown.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Browsing Activities Currently Stored	This query viewer shows the dangerous browsing activities by internal hosts currently stored in a list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
All Communication Events from Malicious Hosts During the Last 7 Days	This query viewer shows all of the inbound communication events from malicious hosts during the last seven days.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Communication Events to Malicious Hosts During the Last 7 Days	This query viewer shows all of the outbound communication events to malicious hosts during the last seven days.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Correlation Events on Dangerous Browsing and Access to Dangerous Destinations	This query viewer shows all correlations events generated by the rules that detect dangerous browsing and access to dangerous destinations.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
All Correlation Events on Zero Day Attacks and Access from Dangerous Sources	This query viewer shows all correlations events generated by the rules that detect zero day attacks and access from dangerous sources.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/

Query Viewers Resources, continued

Resource	Description	URI
All Events to or from Internal IP Addresses Found in Reputation Data within the Last 24 Hours	This query viewer shows all events related to IP addresses found in reputation data.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
All Events with Host Name Information within the Last 24 Hours - Drilldown Only	This query viewer shows all events with host name information during last 24 hours and should be used for drilldown purpose only.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
All Inbound and Outbound Communication Related to Infected Assets During the Last 24 Hours	This query viewer shows all inbound and outbound traffic to or from an infected asset during the last 24 hours.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Infection Base Events During the Last 24 Hours	This query viewer shows all events during the last 24 hours and should only be used for drilldown purposes.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Internal Communication related to Infected Assets During the Last 24 Hours	This query viewer shows all internal traffic to or from an infected asset during the last 24 hours.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
All Internal Domains and Hosts Found	This query viewer shows all local domain names and hosts appeared in the reputation domain database.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
All Internal IP Addresses Found	This query viewer shows all local IP addresses that appear in the reputation domain database.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Query Viewers Resources, continued

Resource	Description	URI
All Occurrences of Access from Dangerous Sources Currently Stored	This query viewer shows the occurrences of access from dangerous sources to internal hosts currently stored in an active list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
All System Events on the Last Day	This query viewer shows system events during the last day.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Zero Day Attacks Currently Stored	This query viewer shows the zero day attacks to internal hosts currently stored in an active list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Assets Infected for More Than a Week	This query viewer shows all infected internal machines that have remained in the infected list over one week.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Address Infection Drilldown Only	This query viewer shows all infection events based on target address during the last 24 hours.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Hostname Infection Drilldown Only	This query returns outbound events during the last 24 hours in which the target host name appears on the malicious domains list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Base Events During the Last 24 Hours - Request Infection Drilldown Only	This query returns outbound events during the last 24 hours in which the request URL appears on the malicious domains list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/

Query Viewers Resources, continued

Resource	Description	URI
Communication from Malicious Hosts	This query viewer displays all inbound malicious communication matches during the last day.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Communication to Malicious Hosts	This query viewer displays all outbound malicious communication matches during the last day.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Currently Infected Assets and Recorded Interactions with Malicious Entities	This query viewer shows all internal infected assets detected through communications with reputation IP addresses or domain names.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Dangerous Destinations Accessed by Internal Assets	This query viewer shows the summary of dangerous destinations contacted by internal hosts.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Dangerous Sites Accessed by Internal Asset	This query viewer shows the summary of dangerous web sites accessed by internal hosts.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Sources	This query viewer shows the dangerous sources accessing internal, non public facing assets, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
Events per Scenario	This query viewer shows the captured events per scenario during the last day.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

Query Viewers Resources, continued

Resource	Description	URI
Infected Asset Count per Month	This query viewer shows the count of internal infected assets per month over the last year.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Infected Assets and Interactions with Malicious Entities During the Last Year	This query viewer shows the list of internal infected assets during the last year.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Internal Assets Accessed by Dangerous Sources	This query viewer shows the summary of internal assets accessed by dangerous sources, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected and the time of the latest attack.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
Internal Assets Communicated with Dangerous Destinations	This query viewer shows the summary of internal assets that communicated with a dangerous destination.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Internal Assets Involved in Dangerous Browsing	This query viewer shows the summary of internal assets involved in dangerous browsing.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Internal Assets Targeted by Zero Day Attacks	This query viewer shows the summary of internal assets targeted by zero day attacks, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected, and the time of the latest attack.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Malicious Communication Matches During the Last 7 Days	This query viewer shows all malicious inbound and outbound communication events during the last seven days, in tabular format.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/

Query Viewers Resources, continued

Resource	Description	URI
Open Case Status Distribution	This query viewer shows all open cases on internal infected assets, grouped by case status.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Open Cases on Zero Day Attacks	This query viewer shows all open cases for zero day attacks.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Reputation Domain Entries	This query viewer shows the top 1,500,000 domain entries in the reputation domain active list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Domain Exploit Type Distribution	This query viewer shows the reputation domain count per exploit type.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Domain Score Histogram	This query viewer shows the histogram of the reputation domain score.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation Domain Type Distribution	This query viewer shows the distribution of entries in the reputation domain database.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/
Reputation IP Entries	This query viewer shows the top 1,500,000 IP entries in the reputation IP active list.	/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/

Query Viewers Resources, continued

Resource	Description	URI
Reputation IP Entry Count	This query viewer shows the current number of reputation addresses.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation IP Exploit Type Distribution	This query viewer shows the reputation address count per exploit type.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation IP Score Histogram	This query viewer shows the histogram of the reputation IP score.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Scenario Matches During the Last 7 Days	This query viewer shows all events related to scenario types captured during the last seven days.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Summary of Contacted Malicious Entities	This query viewer shows the summary of malicious hosts contacted by infected internal hosts.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Summary of Infected Assets	This query viewer shows the summary of internal infected machines detected through communications with reputation IP addresses or domains.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Summary of Open Cases	This query viewer shows the list of open cases on internal infected assets.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`

Query Viewers Resources, continued

Resource	Description	URI
Top 20 Internal Assets with Malicious Communication Matches	This query viewer shows the top 20 internal assets with the most the malicious communication matches during the last seven hours.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Trend of Access from Dangerous Sources	This query viewer shows the daily number of dangerous access events during the last seven days. It is based on a trend so it might not show most recent data.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`
Trend of Access to Dangerous Destinations	This query viewer shows the top daily count of communications with dangerous destinations (domain, host name or IP address) during the last seven days. It is based on a trend so it might not show most recent data.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/`
Trend of Dangerous Browsing Activities During the Last 7 Days	This query viewer shows the top daily count of dangerous browsing activities (based on target domain, host name or IP address) during the last seven days. It is based on a trend so it might not show most recent data.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/`
Trend of Zero Day Attacks	This query viewer shows the daily count of zero day attacks during the last seven days. It is based on a trend so it might not show most recent data.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attack Cases	This query viewer shows all open cases for zero day attacks, grouped by case status.	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attackers	This query viewer shows the sources of zero day attacks, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time	`/All Query Viewers/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`

Reports

The following table lists all the reports.

Reports Resources

Resource	Description	URI
All Events for which a Scenario was Identified	This report shows detailed information about all scenario matches during the last seven days. The information includes the event count per scenario during the last day in a pie chart and all the captured Scenario events during the last seven days in tabular format.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
All Inbound and Outbound Malicious Communication during the Last 7 Days	This report shows detailed information about events with malicious communication during the last seven days.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Assets Infected for More Than A Week	This report shows all infected internal machines that have remained in the infection list for over one week. This might mean that the related cases have not yet been investigated or are still being investigated. By default, when a case on internal infection asset is deleted or closed, the related asset will be removed from the infection list.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Currently Infected Assets and Recorded Interactions with Malicious Entities	This report shows the internal assets that are considered to be infected through their communications with external malicious hosts.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Dangerous Browsing Activities - 30 Day Trend	This report provides information about dangerous browsing activities by internal assets during the last 30 days.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities - One Year Trend	This report provides information about dangerous browsing activities by internal assets during the last year.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities During the Last 24 Hours - Long Form	This report provides information about browsing activities by internal assets to malicious destinations during the last 24 hours.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Dangerous Browsing Activities During the Last 24 Hours - Short Form	This report provides information about browsing activities by internal assets to malicious destinations during the last 24 hours. It shows less data than the longer counterpart.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/

Reports Resources, continued

Resource	Description	URI
Dangerous Browsing Activities During the Last 7 Days	This report provides information about dangerous browsing activities by internal assets during the last seven days.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Interactions with Malicious Entities During the Last 24 Hours	This report shows all interactions with certain malicious entities by internal assets. These assets are then considered infected. Note that an internal asset might be involved in multiple interactions, depending on its communications, but will be reported under a single case.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Internal Assets Found in Reputation Data	This report shows the list of internal IP addresses and internal domain names found in reputation data.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/
List of Internal Assets with Malicious Communication during the last 7 Days	This report shows information about all internal assets with malicious communication during the last seven days.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Malicious Communication Trend over Time of the Last Day	This report shows an overview of captured malicious communication during the last day, and shows the Inbound and Outbound trends over time and the scenario events captured. The report includes communication from malicious hosts during the last day in a bar chart, communication to malicious hosts during the last day in a bar chart, and scenario type events during the last day in tabular format.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Overview of Infected Assets During the Last 30 Days	This report shows an overview of internal infections over the last one month (up to and including yesterday). Its content is based on a daily trend which stores the daily snapshot of the Infected Internal Assets active list.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infection Assets/
Reputation Database Changes During the Last 1 Week	This report shows the reputation domain and IP database changes during the last week.	/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/

Reports Resources, continued

Resource	Description	URI
Reputation Database Changes During the Last 1 Week - Exploit Type Specific	This report shows the changes of a specific reputation exploit type during the last week.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation Database Changes During the Last 1 Year	This report shows the reputation domain and IP database changes during the last year.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation Database Changes During the Last 1 Year - Exploit Type Specific	This report shows the changes of a specific reputation exploit type during the last year.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Zero Day Attacks - 30 Day Trend	This report provides information about zero day attacks by malicious entities on internal assets during the last 30 days. Do not change the default value for the custom parameter AttackType.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks - One Year Trend	This report provides information about zero day attacks to internal assets during the last year. Do not change the default value for the custom parameter AttackType.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks During the Last 24 Hours	This report provides information about zero day attacks to internal assets during the last 24 hours.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`
Zero Day Attacks During the Last 7 Days	This report provides information about zero day attacks on internal assets during the last seven days. Do not change the default value for the custom parameter AttackType.	`/All Reports/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/`

Rules

The following table lists all the rules.

Rules Resources

Resource	Description	URI
Access from Dangerous Sources: Inbound Communications from Malicious Domains	This rule captures inbound communications to internal, from reputation domain names. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious Domain.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/Access from Dangerous Sources/
Access from Dangerous Sources: Inbound Communications from Malicious IPs	This rule captures the inbound communication to internal, from reputation IP addresses. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious IP.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/Access from Dangerous Sources/
Access from Dangerous Sources: Successful Inbound Communications from Malicious Address	This rule captures all successful inbound communications from reputation IP addresses not already captured as zero day attacks. These are flagged as access from dangerous sources.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
Access from Dangerous Sources: Successful Inbound Communications from Malicious Domain	This rule captures events of all successful inbound communications to internal, public-facing assets from reputation domain names without zero day attack exploit types.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/
Access to Dangerous Destinations: Outbound Communications to Malicious Domains	This rule captures all outbound traffic from non public-facing assets to reputation domain names with high scores and non-critical exploit types.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Access to Dangerous Destinations: Outbound Communications to Malicious Domains	This rule captures all outbound traffic from internal assets to reputation domain names. The rule generates a correlated event with the scenario type Outbound Communication to Malicious Domains.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/Access to Dangerous Destinations/

Rules Resources, continued

Resource	Description	URI
Access to Dangerous Destinations: Outbound Communications to Malicious IPs	This rule captures all outbound traffic from non public-facing assets to reputation IP addresses with high scores and non-critical exploit types.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Access to Dangerous Destinations: Outbound Communications to Malicious IPs	This rule captures all outbound traffic from internal assets to reputation IP addresses. The rule generates a correlated event with the scenario type Outbound Communication to Malicious IPs.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/Access to Dangerous Destinations/
Access to Dangerous Destinations: Outbound Requests to Malicious Domains	This rule captures all outbound URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Access to Dangerous Destinations: Outbound Requests to Malicious Domains	This rule captures all outbound URL requests from internal assets to reputation domain names. The rule generates a correlated event with the scenario type Outbound Requests to Malicious Domains.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/Access to Dangerous Destinations/
Dangerous Browsing	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types. Severity is low if the bad host has a type of malware and its score is 40. Otherwise, the severity is high.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Dangerous Browsing/
Infected Internal Assets: Outbound Communications to Malicious Domains	This rule captures all outbound traffic either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain names.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Infected Internal Assets: Outbound Communications to Malicious IPs	This rule captures all outbound traffic either from internal assets to reputation IP addresses with high scores and critical exploit types, or from public-facing assets to any reputation IP.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/

Rules Resources, continued

Resource	Description	URI
Infected Internal Assets: Outbound Requests to Malicious Domains	This rule captures all outbound URL requests either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain names.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Internal Domain Found in Reputation Data	This rule detects when an internal domain appears in the reputation domain database.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Internal IP Address Found in Reputation Data	This rule detects when an internal address appears in the reputation IP database.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Internal Infected Asset Removal on Case Closed or Deleted	This rule removes the relevant internal infected asset when the related case is closed or deleted.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Outbound Communications to Malicious Domains - Detected Instance Update	This lightweight rule captures all outbound traffic either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain names that the main rule skipped.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Outbound Communications to Malicious IPs - Detected Instance Update	This lightweight rule captures all outbound traffic either from internal assets to reputation IP addresses with high scores and critical exploit types, or from public-facing assets to any reputation IP address that the main rule skipped.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Outbound Requests to Malicious Domains - Detected Instance Update	This lightweight rule captures subsequent outbound URL requests either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain names that the main rule skipped.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/`
Peer To Peer	This rule detects a P2P network use threat and creates a correlation event with the scenario type of either Peer To Peer - Inbound Communication or Peer To Peer - Outbound Communication. Event priority depends on the communication outcome.	`/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`

Rules Resources, continued

Resource	Description	URI
Port Scan	The rule detects multiple accesses to different ports from the same dangerous external source. The rule generates a correlation event with the scenario type of Port Scan.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Potential Intrusion	The rule detects multiple accesses from the same bad external source to the same non public-facing host and generates a correlation event with the scenario type of Potential Intrusion.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Potential Spear Phishing	This rule detects spam from malicious sources and creates a correlation event with the scenario type of Potential Spear Phishing.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/
Zero Day Attack Record Removal on Case Closed or Deleted	This rule removes the relevant internal asset when the related case is closed or deleted.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks: Successful Inbound Communications from Malicious Address	This rule captures all successful inbound communications to assets categorized as internal, non public-facing from reputation IP addresses with zero day attack exploit types. These are flagged as potential zero day attacks.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks: Successful Inbound Communications from Malicious Address - First Occurrence	This rule captures the first event of all successful inbound communications to assets categorized as internal, non public-facing from reputation IP addresses with a zero day attack exploit type. It will open a case for each internal target.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks: Successful Inbound Communications from Malicious Domain	This rule captures all successful inbound communications to assets categorized as internal, non public-facing from reputation domain names with zero day attack exploit types. These are flagged as potential zero day attacks.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/
Zero Day Attacks: Successful Inbound Communications from Malicious Domain - First Occurrence	This rule captures the first event of all successful inbound communications to assets categorized as internal, non public-facing from reputation domain names with zero day attack exploit types. It will open a case for each internal target.	/All Rules/ArcSight Solutions/Reputation Security Monitor Plus/Zero Day Attacks/

Rules Resources, continued

Resource	Description	URI
Error in RepSM Plus MIC Service Message	This rule is triggered when the repsm mic has an error to receive or process a malicious list.	/All Rules/Real-time Rules/Reputation Security Monitor Plus/Monitor RepSM MIC Health/Error in RepSM Plus MIC Service Message
No Update from RepSM Plus MIC	This rule will be triggered if any entry expires from the Track RepSM MIC list, which means there is no update from MIC for a certain time period (defined by active list TTL)	/All Rules/Real-time Rules/Reputation Security Monitor Plus/Monitor RepSM MIC Health/No Update from RepSM Plus MIC
Dangerous IP Address Browsing	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation IP address with high scores and non-critical exploit types.	/All Rules/Real-time Rules/Reputation Security Monitor Plus/Dangerous Browsing
Track RepSM Plus MIC Service Message	This rule tracks RepSM Plus MIC service message events, and adds to an active list.	/All Rules/Real-time Rules/Reputation Security Monitor Plus/Monitor RepSM MIC Health

Trends

The following table lists all the trends.

Trends Resources

Resource	Description	URI
Daily Internal Infected Asset Snapshots	This trend stores snapshots of the internal infected asset list on a daily basis.	/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Internal Infected Assets/
Dangerous Browsing and Interactions to Dangerous Destinations	This trend stores firings of rules that detect interactions to all dangerous destinations (browsing and non-browsing types).	/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Access to Dangerous Destinations/
Internal Asset Reputation Detector (Asset Based)	This trend detects internal assets in the asset model that appear in the reputation IP list.	/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/

Trends Resources, continued

Resource	Description	URI
Internal Asset Reputation Detector (List Based)	This trend stores all internal hosts that appear in the reputation IP database. It runs on the reputation database and correlates with a list of local addresses to be monitored. All found internal bad assets will be stored in an active list.	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Internal Domain Reputation Detector (List Based)	This trend detects all internal domain names that appear in the reputation domain list. It runs on top of the reputation domain list and correlates with a given set of domain names to be monitored.	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Internal Assets Found in Reputation Data/`
Layer 1 Trend	This trend runs hourly over Layer 1 events (Inbound/Outbound Malicious Communication).	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Layer 2 Trend	This trend runs hourly over Layer 2 events (Scenario events).	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/General Scenarios/`
Reputation Domain Changes	This trend stores the daily count of reputation domain names, grouped by the exploit type.	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Reputation IP changes	This trend stores the daily count of reputation IP entries, grouped by the exploit type.	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Reputation Data Analysis/`
Zero Day Attacks and Access from Dangerous Sources	This trend stores all triggerings of rules that detect zero day attacks or access from dangerous sources.	`/All Trends/ArcSight Solutions/Reputation Security Monitor Plus/Access from Dangerous Sources/`

Use Cases

The following table lists all the use cases.

Use Cases Resources

Resource	Description	URI
Dangerous Browsing	This use case shows all dangerous browsing.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
Event Enrichment with Reputation Data	This use case contains resources that can be combined with your existing resources to show reputation information and provide better context for investigating issues..	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
General Scenarios	The General Scenarios use case provides resources that focus on inbound and outbound malicious communication identified by scenarios, during the last seven days.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
Internal Assets Found in Reputation Data	This use case shows information about internal assets (including domain names) that appear in the reputation database. These assets should be examined and monitored carefully.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
Internal Infected Assets	This use case provides information around internal assets that either: (a) are public-facing and communicating with any malicious entity or (b) are not public-facing and communicating with malicious entities with critical exploit types. These critical types are defined in the Critical Exploit Types active list. For either case, only malicious entities with scores over a certain threshold are considered.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
RepSM Overview	This use case shows overview information related to detected reputation traffic.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
RepSM Package Health Status	This use case shows information around the health of important resources in the Reputation Security Monitor package.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
Reputation Data Analysis	This use case shows information around the reputation database, including IP addresses and domain or host names.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/
Zero Day Attacks	This use case provides information about successful communications that might indicate potential attacks from malicious sources.	/All Use Cases/ArcSight Solutions/Reputation Security Monitor Plus/

Send Documentation Feedback

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

Feedback on Solutions Guide (ESM RepSM Plus 1.8)

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!