



**Hewlett Packard**  
Enterprise

## **Solution Guide**

HPE Reputation Security Monitor 1.52

March 31, 2017

## Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice

© Copyright 2017 Hewlett Packard Enterprise Development LP

Follow this link to see a complete statement of copyrights and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>

## Contact Information

---

|                              |   |
|------------------------------|---|
| <b>Phone</b>                 | A list of phone numbers for HPE ArcSight Technical Support is available on the HPE Enterprise Security contacts page:<br><a href="http://www.hpe.com/software/support/contact_list">www.hpe.com/software/support/contact_list</a> |
| <b>Support Web Site</b>      | <a href="http://www.hpe.com/software/support">www.hpe.com/software/support</a>  |
| <b>Protect 724 Community</b> | <a href="https://www.protect724.hpe.com">https://www.protect724.hpe.com</a>   |

---

# Contents

---

|   |           |
|---|-----------|
| <b>Chapter 1: Overview and Architecture</b>           | <b>7</b>  |
| How RepSM Works                                       | 7         |
| What RepSM Can Do for You                             | 8         |
| Protect from Advanced Persistent Threats (APTs)       | 8         |
| Detect and Analyze Zero Day Attacks                   | 8         |
| Provide Insight into Malicious Communication          | 9         |
| Ensure the Reputation of Your Organization's Assets   | 9         |
| Optimize the Security Operations Center               | 9         |
| Reputation Data                                       | 9         |
| Reputation Scores                                     | 9         |
| Exploit Types   | 10        |
| RepSM Scenarios                                       | 10        |
| Integration Commands                                  | 12        |
| Pattern Discovery                                     | 12        |
| Supported Devices                                     | 12        |
| <b>Chapter 2: Installing and Configuring RepSM</b>    | <b>13</b> |
| Installation Overview                                 | 13        |
| Verifying Your Environment                            | 13        |
| Configuring the Active List Capacity (Required)       | 14        |
| Installing the RepSM Content                          | 14        |
| Troubleshooting Your Installation                     | 17        |
| Installing the Model Import Connector for RepSM       | 17        |
| Configuring the RepSM Content                         | 17        |
| Assigning User Permissions                            | 18        |
| Including and Excluding Entries from Reputation Data  | 19        |
| Using the RepSM Event Limit Filter                    | 20        |
| Configuring Internal Assets Found in Reputation Data  | 20        |
| Configuring Exploit Types                             | 20        |
| Categorizing Assets                                   | 21        |
| How to Assign Asset Categories                        | 21        |
| Deploying Rules                                       | 22        |
| Configuring Integration Commands                      | 22        |
| Configuring the TippingPoint SMS Integration Commands | 22        |

|   |           |
|---|-----------|
| Configuring the Web Search Integration Command .....    | 23        |
| Setting Thresholds for the Reputation Score .....       | 23        |
| Creating Custom Scenarios .....                         | 25        |
| Enabling Trends .....                                   | 26        |
| Configuring Cases .....                                 | 26        |
| Verifying RepSM Content Configuration .....             | 26        |
| <b>Chapter 3: Using RepSM Content .....</b>             | <b>27</b> |
| Best Practices .....                                    | 29        |
| Manage Cases to Ensure Continued Detection .....        | 29        |
| Get Email About RepSM Service Outages .....             | 29        |
| Start With a Host Name or Domain Name .....             | 29        |
| Use the Integrated Web Search for Malicious Hosts ..... | 29        |
| Use Pattern Discovery in Your Investigation .....       | 30        |
| Sort Displays to Prioritize Your Investigation .....    | 30        |
| Use the TippingPoint Integration Commands .....         | 30        |
| RepSM Overview .....                                    | 32        |
| Configuration .....                                     | 32        |
| Usage .....   | 32        |
| General Scenarios .....                                 | 34        |
| Configuration .....                                     | 34        |
| Usage .....   | 34        |
| Key Resources .....                                     | 35        |
| Internal Infected Assets .....                          | 37        |
| Configuration .....                                     | 37        |
| Usage .....   | 38        |
| Key Resources .....                                     | 39        |
| Zero Day Attacks .....                                  | 42        |
| Configuration .....                                     | 42        |
| Usage .....   | 42        |
| Key Resources .....                                     | 44        |
| Dangerous Browsing .....                                | 46        |
| Configuration .....                                     | 46        |
| Usage .....   | 46        |
| Key Resources .....                                     | 48        |
| Internal Assets Found in Reputation Data .....          | 50        |
| Configuration .....                                     | 50        |
| Usage .....   | 51        |
| Key Resources .....                                     | 52        |
| Event Enrichment with Reputation Data .....             | 54        |
| Configuration .....                                     | 54        |
| Usage .....   | 54        |
| Key Resources .....                                     | 54        |

---

|   |           |
|---|-----------|
| RepSM Package Health Status .....                         | 57        |
| Configuration .....                                       | 57        |
| Usage .....   | 57        |
| Key Resources .....                                       | 58        |
| Reputation Data Analysis .....                            | 60        |
| Configuration .....                                       | 60        |
| Usage .....   | 60        |
| Key Resources .....                                       | 61        |
| <b>Appendix A: Troubleshooting .....</b>                  | <b>63</b> |
| <b>Appendix B: Upgrading and Uninstalling RepSM .....</b> | <b>67</b> |
| Upgrade from RepSM 1.5 .....                              | 67        |
| Stop the Model Import Connector for RepSM .....           | 67        |
| Identify Customized Resources .....                       | 68        |
| Back Up the Reputation Data Active Lists .....            | 68        |
| Back Up RepSM 1.5 .....                                   | 70        |
| Uninstall RepSM 1.5 .....                                 | 71        |
| Install RepSM 1.52 .....                                  | 72        |
| Import the Backed Up Active Lists .....                   | 72        |
| Customize the RepSM 1.52 Resources .....                  | 72        |
| Install the Model Import Connector for RepSM .....        | 73        |
| Start the Model Import Connector for RepSM .....          | 73        |
| <b>Appendix C: RepSM Service Messages .....</b>           | <b>75</b> |
| Service Activation Messages .....                         | 75        |
| Data Retrieval Messages .....                             | 76        |
| <b>Appendix D: RepSM Resource Reference .....</b>         | <b>77</b> |
| Dangerous Browsing .....                                  | 77        |
| Event Enrichment with Reputation Data .....               | 90        |
| General Scenarios .....                                   | 95        |
| Internal Assets Found in Reputation Data .....            | 98        |
| Internal Infected Assets .....                            | 100       |
| RepSM Overview .....                                      | 111       |
| RepSM Package Health Status .....                         | 124       |
| Reputation Data Analysis .....                            | 143       |
| Zero Day Attacks .....                                    | 148       |



# Chapter 1

## Overview and Architecture

---

This chapter discusses the following topics:

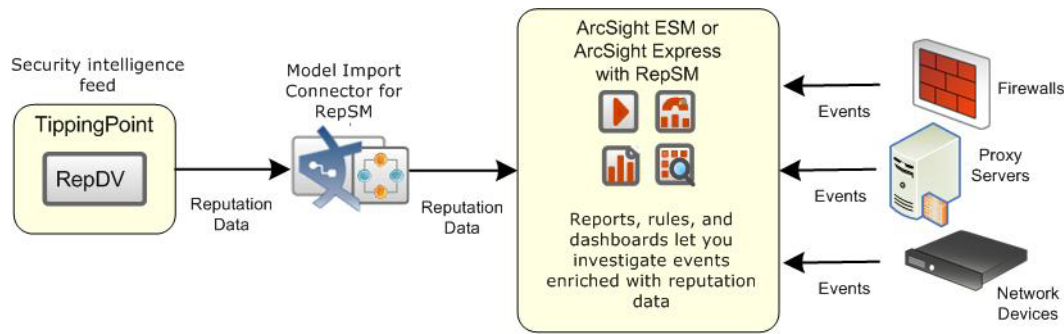
- [“How RepSM Works” on page 7](#)
- [“What RepSM Can Do for You” on page 8](#)
- [“Reputation Data” on page 9](#)
- [“RepSM Scenarios” on page 10](#)
- [“Integration Commands” on page 12](#)
- [“Pattern Discovery” on page 12](#)
- [“Supported Devices” on page 12](#)

### How RepSM Works

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

- The HPE RepSM service, powered by TippingPoint Reputation Digital Vaccine (RepDV), provides reputation data from the comprehensive RepDV database of malicious IP addresses, host names, and domain names. RepDV uses IPv4 and Domain Name System (DNS) security intelligence feeds from multiple sources to provide a broad set of reputation data.
- The HPE Model Import Connector for RepSM imports the reputation data at regular intervals from the RepSM service to ArcSight ESM or ESM Express.
- The HPE RepSM 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 content is organized into several use cases, which address specific objectives.

The following figure shows how the RepSM components work together.



## What RepSM Can Do for You

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

- [“Protect from Advanced Persistent Threats \(APTs\)” on page 8](#)
- [“Detect and Analyze Zero Day Attacks” on page 8](#)
- [“Provide Insight into Malicious Communication” on page 9](#)
- [“Ensure the Reputation of Your Organization’s Assets” on page 9](#)
- [“Optimize the Security Operations Center” on page 9](#)

### 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 enables you to:

- Detect APTs early by correlating events regarding communication from internal computers to external command and control centers.
- Mitigate attacks by using the HPE TippingPoint integration commands to quarantine infected computers.
- 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. For more information, see [“Internal Infected Assets” on page 37](#).

### 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 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. For more information about the use case, see [“Zero Day Attacks” on page 42](#).



## Provide Insight into Malicious Communication

RepSM 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 Scenarios” on page 10](#).

The **General Scenarios** use case provides a dashboard of inbound and outbound malicious communication during the last seven days. For more information about the use case, see [“General Scenarios” on page 34](#).

## Ensure the Reputation of Your Organization’s Assets

RepSM 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. For more information about the use case, see [“Internal Assets Found in Reputation Data” on page 50](#).

## Optimize the Security Operations Center

RepSM 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 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 resources. For more information, see [“Event Enrichment with Reputation Data” on page 54](#).

## Reputation Data

RepSM stores the reputation data from the RepSM service in active lists; one list for IP addresses and another list for host names and domain names. Those active lists are collectively referred to as the *reputation database*. Each IP address, host name, or domain name in the reputation database has a *reputation score* and *exploit type*, as described in the following sections. The RepSM 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 19](#).

## 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 RepDV. 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.



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 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:

|                                 |  |
|---------------------------------|--|
| <b>Blended Threat</b>           | The malicious host is classified as having multiple exploit types.   |
| <b>Botnet</b>                   | The malicious host is either a member of a botnet or a command and control center for a botnet.  |
| <b>Malware</b>                  | The malicious host is one of the following: <ul style="list-style-type: none"><li>• A web server that distributes malware to users who browse sites located on the server.</li><li>• A command and control center for computers infected with malware.</li></ul> |
| <b>Miscellaneous</b>            | The host is considered malicious, but there is insufficient information to classify it as another, more specific exploit type.   |
| <b>Misuse and Abuse</b>         | The malicious host scans the internet for vulnerable systems, or serves adult content.   |
| <b>P2P</b>                      | 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.  |
| <b>Phishing</b>                 | The malicious host sends phishing emails, or the malicious host's URL appears in the text of phishing emails.  |
| <b>Spam</b>                     | The malicious host sends spam emails.  |
| <b>Spyware</b>                  | The malicious host distributes spyware or other suspicious software.   |
| <b>Web Application Attacker</b> | The malicious host initiates application layer attacks, such as SQL injection and Cross Site Scripting, against web servers.   |
| <b>Worm</b>                     | The malicious host is infected by a worm.  |

## RepSM Scenarios

RepSM 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. 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 [“Creating Custom Scenarios” on page 25](#).

| Scenario                 | Direction of Communication                  | Outcome of Communication | Malicious Host Exploit Type  | Asset or Activity Detected   |
|--------------------------|---|--------------------------|--|--|
| Internal Infected Assets | Outbound to malicious host                  | Success and failure      | Botnet   | Assets <b>not</b> categorized as Public-Facing <sup>a</sup>  |
|                          |   |                          | All exploit types <sup>b</sup>   | Assets categorized as Public-Facing  |
| Zero Day Attacks         | Inbound from malicious host                 | Success                  | Botnet, Miscellaneous, Misuse and Abuse, Web Application Attacker, Worm                          | Assets categorized as Internal Non Public-Facing   |
| Dangerous Browsing       | Outbound to malicious host                  | Success and failure      | Phishing, Malware  | Assets <b>not</b> categorized as Public-Facing <sup>a</sup> and events that have a URL request and the port is 80 or 443                                   |
| 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 <b>different</b> ports |
| Potential Spear Phishing | Inbound from malicious host                 | Success and failure      | Phishing, Spam   |  |
| Peer-to-Peer             | Inbound from and outbound to 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 <b>same</b> port   |

a.If you classify assets in this category, 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.

b.For a complete list of exploit types, see [“Exploit Types” on page 10](#).

## Integration Commands

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

- The HPE TippingPoint Security Management System (SMS) commands quarantine an infected asset and unquarantine it after the issue is resolved.
- The ArcSight Logger commands query historical activity of infected assets.
- The Google web search command finds information about a malicious host.

For more information about these integration commands, see [“Configuring Integration Commands” on page 22](#).

## Pattern Discovery

RepSM 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 30](#).

## 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 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 and Configuring RepSM

---

This chapter describes how to install and configure the RepSM solution and discusses the following topics.

[Installation Overview](#), described below

[“Verifying Your Environment” on page 13](#)

[“Configuring the Active List Capacity \(Required\)” on page 14](#)

[“Installing the RepSM Content” on page 14](#)

[“Installing the Model Import Connector for RepSM” on page 17](#)

[“Configuring the RepSM Content” on page 17](#)

## Installation Overview

Perform the installation tasks in the following order:

- 1 Verify your ArcSight environment. See [“Verifying Your Environment” on page 13](#).
- 2 Increase the maximum capacity for active lists. See [“Configuring the Active List Capacity \(Required\)” on page 14](#).
- 3 Install the content package (.arb file). See [“Installing the RepSM Content” on page 14](#).
- 4 Install the Model Import Connector for RepSM. See [“Installing the Model Import Connector for RepSM” on page 17](#).
- 5 Configure the RepSM content. Minimally, you must deploy the RepSM rules to ensure that the use cases produce results. See [“Configuring the RepSM Content” on page 17](#).

## Verifying Your Environment

Before you install RepSM, make sure that you are running a supported version of ArcSight ESM or ArcSight Express.



The ArcSight ESM Manager Java heap memory size must be set to at least 4 GB to support RepSM. For information about setting the heap size, see the ArcSight ESM *Installation and Configuration Guide*.

For ArcSight Express, the Java heap memory size is set to support RepSM.

## Configuring the Active List Capacity (Required)

Before you install the RepSM content on either ArcSight ESM or ArcSight Express, the active list capacity must be increased to 1,500,000 to enable RepSM to monitor that number of reputation data entries. Otherwise, the installation of the RepSM 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 on ArcSight ESM or ArcSight Express. If you encounter this error, see [“Troubleshooting Your Installation” on page 17](#) for additional information.

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 appropriate *ArcSight Administrator's Guide*.

## Installing the RepSM Content

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

If you are upgrading from the previous version of RepSM, see [Appendix B, Upgrading and Uninstalling RepSM, on page 67](#).



Note

The RepSM content is a self-contained solution that does not rely on any other ArcSight solution. You can install the RepSM content package alongside other solutions on the same ArcSight Manager. Before installing a new solution, HPE recommends that you back up any existing solutions installed on the ArcSight Manager. For detailed instructions, see [Appendix B, Upgrading and Uninstalling RepSM, on page 67](#).

---

### To install the RepSM content package:

- 1 Make sure the maximum capacity for active lists is set to 1,500,000, as described in [“Configuring the Active List Capacity \(Required\)” on page 14](#).
- 2 Download the following RepSM content package bundle to the machine where you plan to run the ArcSight Console:

`ArcSight-SolutionPackage-RepSM.1.52<nnnn>.0.arb`

Where `<nnnn>` is the 4 character build number specified in the Reputation Security Monitor Release Notes.



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.

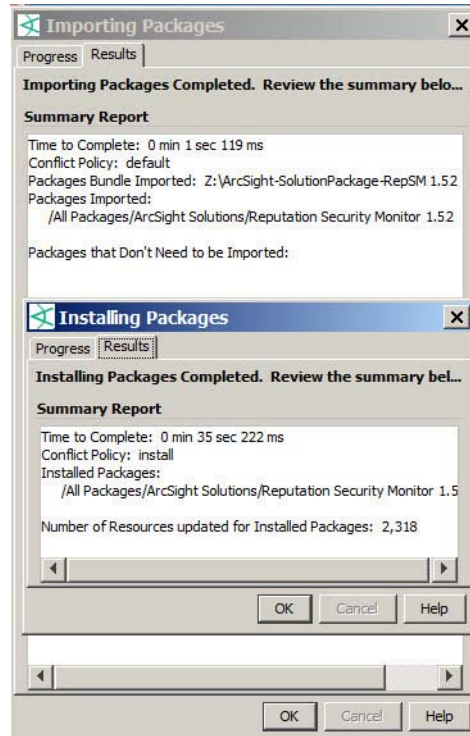
---

- 3 Log into the ArcSight Console with an account that has administrative privileges.

- 4 In the Navigator panel, click the **Packages** tab.
- 5 Click **Import** (↓).
- 6 In the Open dialog, browse and select the package bundle file, and then select Open.

The Progress tab of the Importing Packages dialog shows how the package bundle import is progressing.

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

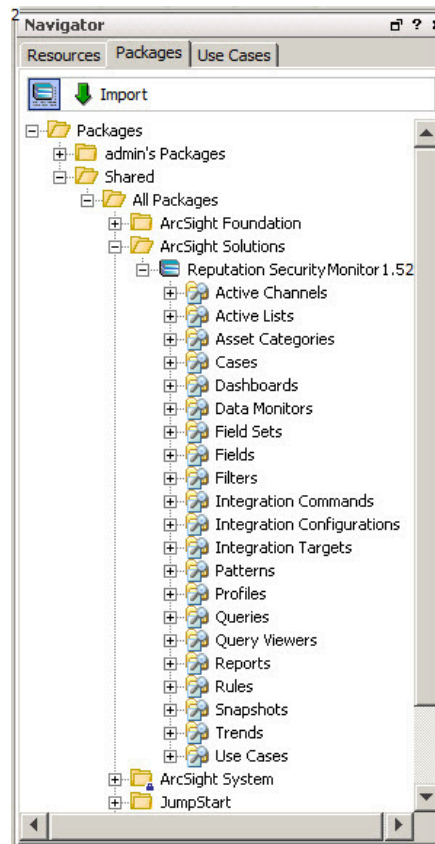


- 7 In the Packages for Installation dialog, leave the Reputation Security Monitor 1.52 checkbox selected and click **Next**.

The Installing Packages dialog opens. The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the Summary Report.

- 8 In the Installing Packages dialog, click **OK**.
- 9 In the Importing Packages dialog, click **OK**.
- 10 On the **Packages** tab of the Navigator panel, expand the Reputation Security Monitor 1.52 group to verify that the installation is successful and that the content

is accessible in the Navigator panel.



**Note**

After you install the RepSM package, perform any required configuration of the RepSM content to ensure that the use cases produce results. For more information, see [“Configuring the RepSM Content” on page 17](#).

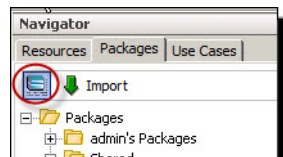


## Troubleshooting Your Installation

If you attempted to install the RepSM content package *before* increasing the active list capacity as described in [“Configuring the Active List Capacity \(Required\)” on page 14](#), and the installation failed, the RepSM 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 1.n
```

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



If the installation is not successful, refer to the contact information on the front inside cover.

For additional, post-installation troubleshooting information, see [Appendix A, Troubleshooting, on page 63](#).



If you need to back up or uninstall the RepSM content at a later date, see [Appendix B, Upgrading and Uninstalling RepSM, on page 67](#).

Note

## Installing the Model Import Connector for RepSM

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

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

For the supported versions of the Model Import Connector for RepSM, see the Reputation Security Monitor Release Notes.

## Configuring the RepSM Content

Several of the RepSM 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 resources. Specific configuration tasks for the RepSM use cases are described in [Chapter 3, Using RepSM Content, on page 27](#).

- [“Assigning User Permissions” on page 18](#)
- [“Including and Excluding Entries from Reputation Data” on page 19](#)
- [“Using the RepSM Event Limit Filter” on page 20](#)

- [“Configuring Internal Assets Found in Reputation Data” on page 20](#)
- [“Configuring Exploit Types” on page 20](#)
- [“Categorizing Assets” on page 21](#)
- [“Deploying Rules” on page 22](#)
- [“Configuring Integration Commands” on page 22](#)
- [“Setting Thresholds for the Reputation Score” on page 23](#)
- [“Creating Custom Scenarios” on page 25](#)
- [“Enabling Trends” on page 26](#)
- [“Configuring Cases” on page 26](#)
- [“Verifying RepSM Content Configuration” on page 26](#)

## Assigning User Permissions

By default, users in the `Default` user group can view RepSM content, and users in the `ArcSight Administrators` and `Analyzer Administrators` user groups have read and write access to the RepSM 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 with an account that has administrative privileges.
- 2 For all the resource types listed above, change the user permissions:
  - a In the Navigator panel, go to the resource type and navigate to `ArcSight Solutions/Reputation Security Monitor 1.5`.
  - b Right-click the Reputation Security Monitor 1.5 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 resources and click **OK**.

## Including and Excluding Entries from Reputation Data

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

You can 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 service:

- Additional Malicious IP Addresses
- Additional Malicious Domains

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 use cases and are located in ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data.

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



Domain names and host 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.

## Using the RepSM Event Limit Filter

RepSM processes events from the devices described in [“Supported Devices” on page 12](#). 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. 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
1.5/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



**Tip**

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 more information, see [“Internal Assets Found in Reputation Data” on page 50](#).

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                                 |
|--|---|
| <a href="#">Critical Exploit Types</a>           | <a href="#">“Internal Infected Assets” on page 37</a> |
| <a href="#">Dangerous Browsing Exploit Types</a> | <a href="#">“Dangerous Browsing” on page 46</a>       |
| <a href="#">Zero Day Attack Exploit Types</a>    | <a href="#">“Zero Day Attacks” on page 42</a>         |

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.

## Categorizing Assets

Categorizing assets adds valuable context to the events evaluated by the RepSM use cases. The RepSM 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).<br><br>By default, any address contained in the Private Address Space Zones is categorized as Protected. | Site Asset<br>Categories/Address Spaces              |
| Public-Facing              | This RepSM asset category classifies internal assets that are accessible from the internet.   | ArcSight<br>Solutions/Reputation<br>Security Monitor |
| Internal Non Public-Facing | This RepSM asset category classifies internal assets that are not accessible from the internet.   | ArcSight<br>Solutions/Reputation<br>Security Monitor |

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 table below.

| Use Case  | Asset Category             | Categorization is: |
|---|----------------------------|--------------------|
| <a href="#">"Dangerous Browsing" on page 46</a>       | Public-Facing              | Recommended        |
| <a href="#">"Internal Infected Assets" on page 37</a> | Public-Facing              | Recommended        |
| <a href="#">"Zero Day Attacks" on page 42</a>         | Internal Non Public-Facing | Required           |

For more information about how categorization affects the use cases, see ["RepSM Scenarios" on page 10](#).

## How to Assign Asset Categories

The RepSM 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 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, see the ArcSight Asset Import SmartConnector Configuration Guide.

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

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

- 1 In the Navigator panel Resources tab, go to Rules and navigate to the ArcSight Solutions/Reputation Security Monitor 1.5 group.
- 2 Right-click the Reputation Security Monitor 1.5 group and select **Deploy Real-time Rule(s)**.

After a few seconds, the rules in the group will be listed under the Real-time Rules/Reputation Security Monitor 1.5 group.

The rules in this group are linked to the rules in the ArcSight Solutions/Reputation Security Monitor 1.5 group.

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

## Configuring Integration Commands

RepSM provides integration commands for TippingPoint SMS and Google. The following sections explain how to configure those commands.

RepSM also provides integration commands for ArcSight Logger searches. For information about configuring and using those commands, see the ArcSight Console User's Guide.

## Configuring the TippingPoint SMS Integration Commands

You can send commands from the ArcSight Console to the TippingPoint SMS appliance to quarantine and unquarantine assets in your network. The SMS login credentials are specified in an integration target, and additional parameters are specified at runtime, when the command is invoked.

The following procedure assumes familiarity with TippingPoint SMS.

### To configure the TippingPoint SMS appliance target:

- 1 In the Navigator panel Resources tab, go to Integration Commands and select the **Targets** tab.
- 2 Navigate to /All Integration Targets/ArcSight Solutions/Reputation Security Monitor 1.5/
- 3 Right-click **TippingPoint SMS Appliance** and select **Edit Target** to open the target in the Inspect/Edit panel.
- 4 Select the **Integration Parameters** tab and enter the IP address, user ID, and password for the SMS appliance in the **Value** column.
- 5 Click **OK** to save the target.

For information about running the commands in the ArcSight Console, see [“Use the TippingPoint Integration Commands” on page 30](#).

## Configuring the Web Search Integration Command

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

- 1 In the Navigator panel Resources tab, go to Integration Commands and select the **Commands** tab.
- 2 Navigate to /All Integration Commands/ArcSight Solutions/Reputation Security Monitor 1.5.
- 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](http://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 reflect your changes.
- 7 Click **OK**.

## Setting Thresholds for the Reputation Score

Several RepSM use cases provide rules that rely on a reputation score threshold. Only IP addresses, host names, 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 threshold is defined in several global variables provided by the use cases, as described in [Table 2-1](#):

**Table 2-1 Reputation Score Threshold Variables**

| Variable   | Use Case  |
|--|---|
| <a href="#">Dangerous Browsing Reputation Domain Score Threshold</a><br><a href="#">Dangerous Browsing Reputation IP Score Threshold</a>             | <a href="#">“Dangerous Browsing” on page 46</a>       |
| <a href="#">Internal Infected Assets Reputation Domain Score Threshold</a><br><a href="#">Internal Infected Assets Reputation IP Score Threshold</a> | <a href="#">“Internal Infected Assets” on page 37</a> |
| <a href="#">Zero Day Attacks Reputation Domain Score Threshold</a><br><a href="#">Zero Day Attacks Reputation IP Score Threshold</a>                 | <a href="#">“Zero Day Attacks” on page 42</a>         |

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

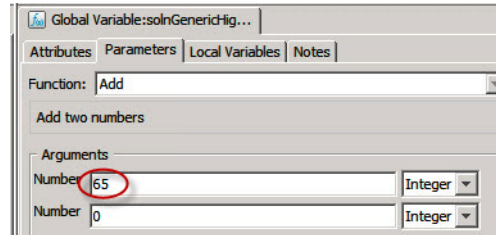
To change the thresholds, you can either set the threshold in the generic variable, which will affect all of the use cases listed in [Table 2-1](#), or you can override the generic variable and specify thresholds in the individual use cases, as described below.

**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:

Fields/Shared/All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration

- 2 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 below:



- 4 Click **OK** to save your changes.

**To set the threshold in an individual use case:**

- 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:

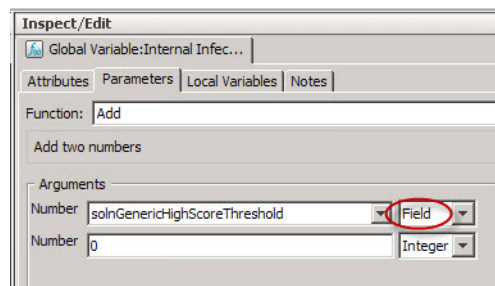
Fields/Shared/All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration

- 2 Double-click the variable to open it in the Inspect/Edit panel. (The variables are listed [Table 2-1 on page 23.](#))
- 3 Click the **Parameters** tab and do **one** of the following:

- ◆ Specify a value in the bottom Number field. That value will be added to the value in the generic variable.

To see the current value of solnGenericHighScoreThreshold, click the pull-down menu, and hover the mouse over the variable in the list.

- ◆ Remove the generic variable by changing Field to Integer, and then specify a value in either of the Number fields.



- 4 Click **OK** to save your changes.



## Creating Custom Scenarios

In addition to the scenarios described in [“RepSM Scenarios” on page 10](#), 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 scenario rules; drag the rule from the All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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:

Shared/All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios

- 2 Add the case sensitive scenario name (that you specified in the Device Custom String6 field in [Step 4](#)) 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 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, go to the Navigator panel, right-click the trend you want to enable and select **Enable 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.

For more information about trends, refer to the the ArcSight Console User's Guide.

## 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 rules create a case if certain conditions are met.

RepSM includes the ArcSight Solutions/Reputation Security Monitor 1.5 group, which holds the cases generated by some RepSM rules.

You can add more groups to the ArcSight Solutions/Reputation Security Monitor 1.5 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 [“Manage Cases to Ensure Continued Detection” on page 29](#).

## Verifying RepSM Content Configuration

After you have finished configuring the RepSM 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 57](#).

## Chapter 3

# Using RepSM Content

---

RepSM provides the use cases listed in the following table.

| Use Case  | Purpose of Use Case  |
|---|--|
| <a href="#">“RepSM Overview” on page 32</a>                           | The RepSM Overview use case provides quick access to the overview dashboards provided by the other RepSM use cases, and is especially helpful if you are unfamiliar with the RepSM content.  |
| <a href="#">“General Scenarios” on page 34</a>                        | The General Scenarios use case provides resources that focus on inbound and outbound malicious communication identified by scenarios.  |
| <a href="#">“Internal Infected Assets” on page 37</a>                 | 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.  |
| <a href="#">“Zero Day Attacks” on page 42</a>                         | 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.                  |
| <a href="#">“Dangerous Browsing” on page 46</a>                       | 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.  |
| <a href="#">“Internal Assets Found in Reputation Data” on page 50</a> | 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. |
| <a href="#">“Event Enrichment with Reputation Data” on page 54</a>    | The Event Enrichment with Reputation Data use case provides resources that let you add reputation data to non-RepSM resources. By enriching those resources with global threat intelligence, security analysts can focus on key events involving known malicious entities.   |

The following use cases provide tools for evaluating the status of the RepSM package and reputation database.

| Use Case   | Purpose of Use Case  |
|--|--|
| <a href="#">“RepSM Package Health Status” on page 57</a> | The RepSM Package Health Status use case provides information about the operational status of important RepSM resources. Various dashboards show the state of important rules and trends; the number of events evaluated by each RepSM use case and the devices that generated those events; and messages from the Model Import Connector for RepSM and the RepSM service. |
| <a href="#">“Reputation Data Analysis” on page 60</a>    | 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.   |

## Best Practices

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

### Manage Cases to Ensure Continued Detection

Some use cases open a case (trouble-ticket) when they detect a potentially compromised asset. The case name includes the address and host name of the asset. When you close or delete the case, the asset is removed from the use case's overview dashboard. If the asset becomes compromised again, a new case is opened, using the same case name.

If you choose to close instead of delete the case, HPE recommends that you move the case to another location to ensure that RepSM detects issues with the asset in the future.

You can access the cases from the Navigator panel Resources tab, by selecting **Cases** from the drop-down list and navigating to:

```
Cases/Shared/All Cases/ArcSight Solutions/Reputation Security
Monitor 1.5
```

### Get Email About RepSM Service Outages

A RepSM service outage can affect the data displayed in several of the use case dashboards. Register for a Protect 724 account so you can sign up to receive email notifications about such outages.

To receive emails, log in to Protect 724, select **Browse > Places** and navigate to the RepSM group, and then click **Receive Email Notifications** in the Actions panel.

### Start With a Host Name or Domain Name

Many of the RepSM use case resources provide reputation data for either IP addresses or host names and domain names. In general, IP addresses indicate clients, while host and domain names indicate servers. Host and 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 host or domain name.

### Use the Integrated Web Search for Malicious Hosts

Throughout the RepSM use cases, you can get information about a malicious host 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.

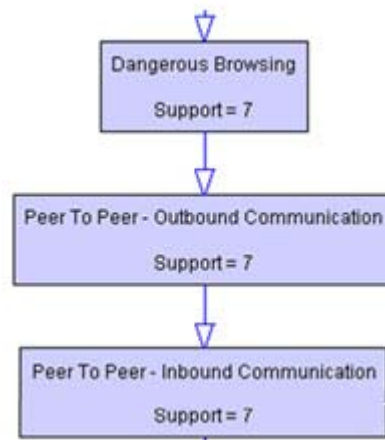
If you think the site is not dangerous, consider deleting its entry from the Malicious Domains or Malicious IP Addresses active lists. To have the site removed more permanently from the reputation data, contact Customer Support. Alternatively, you can identify the site

in an exception active list, as described in [“Including and Excluding Entries from Reputation Data” on page 19](#).

## Use Pattern Discovery in Your Investigation

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

For example, the Complex Attacks Investigation profile might reveal that a user browsed a malicious web site and then started to receive unsolicited, suspicious emails:



The support value in each node is the number of times the event occurred.

To get started, select **Pattern Discovery** in the Navigator panel, navigate to All Profiles/ArcSight Solutions/Reputation Security Monitor 1.5, 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.

## Use the TippingPoint Integration Commands

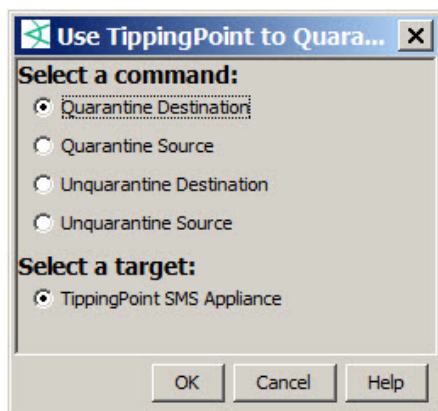
You can send commands from the ArcSight Console to the TippingPoint SMS appliance to quarantine and unquarantine assets in your network. Before you can use the commands, the SMS login credentials must be provided in an integration target, as described in [“Configuring the TippingPoint SMS Integration Commands” on page 22](#).

The following procedure assumes familiarity with TippingPoint SMS.

### To run the TippingPoint integration commands:

- 1 In a RepSM dashboard, right-click an internal asset and select **Integration Commands > Use TippingPoint to Quarantine**.

- 2 Select a destination or source command in the dialog shown below, depending on whether the internal asset is the destination or source of the malicious communication. For inbound communication, the asset is typically the destination; for outbound communication, the asset is typically the source of the communication.



- 3 Click **OK**.
- 4 In the dialog shown below, specify the parameter values in the **Value** column:

| Save To Target           | Save To User             | Parameter          | Type | Value |
|--------------------------|--------------------------|--------------------|------|-------|
| <input type="checkbox"/> | <input type="checkbox"/> | destinationAddress | Text |       |
| <input type="checkbox"/> | <input type="checkbox"/> | Quarantine Timeout | Text |       |
| <input type="checkbox"/> | <input type="checkbox"/> | Policy             | Text |       |

The parameters are:

**destinationAddress** - If the asset you selected in the dashboard shows a Destination Address field, that address is used, and this parameter is not displayed in the dialog. Otherwise, type the address of the asset.

**sourceAddress** - If the asset you selected in the dashboard shows a Source Address field, that address is used, and this parameter is not displayed in the dialog. Otherwise, type the address of the asset.

**Quarantine Timeout** - The number of minutes the asset will remain in quarantine. (This parameter is not applicable to the Unquarantine command.)

**Policy** - The name of an existing TippingPoint SMS quarantine policy to use for the quarantine. The name is case sensitive and can contain spaces. (This parameter is not applicable to the Unquarantine command.)

If you have appropriate permissions, you can save parameter values to the integration target or with your user account so you do not have to re-type them each time you run the command.

- 5 Click **OK**.

The command and parameters are sent to the TippingPoint SMS appliance. You can view the results of the command on the SMS console.

## RepSM Overview

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

## Configuration

No configuration is required for this use case.

## Usage

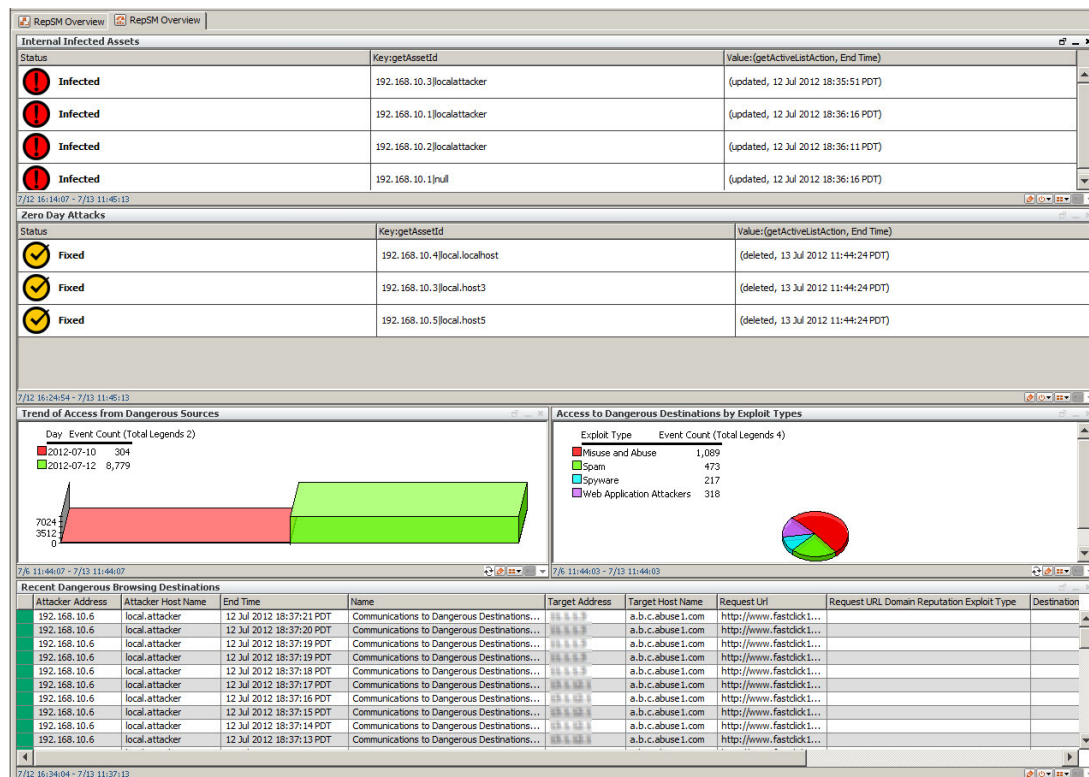
To get started:

- 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 1.5

- 2 Open the [RepSM Overview](#) dashboard.

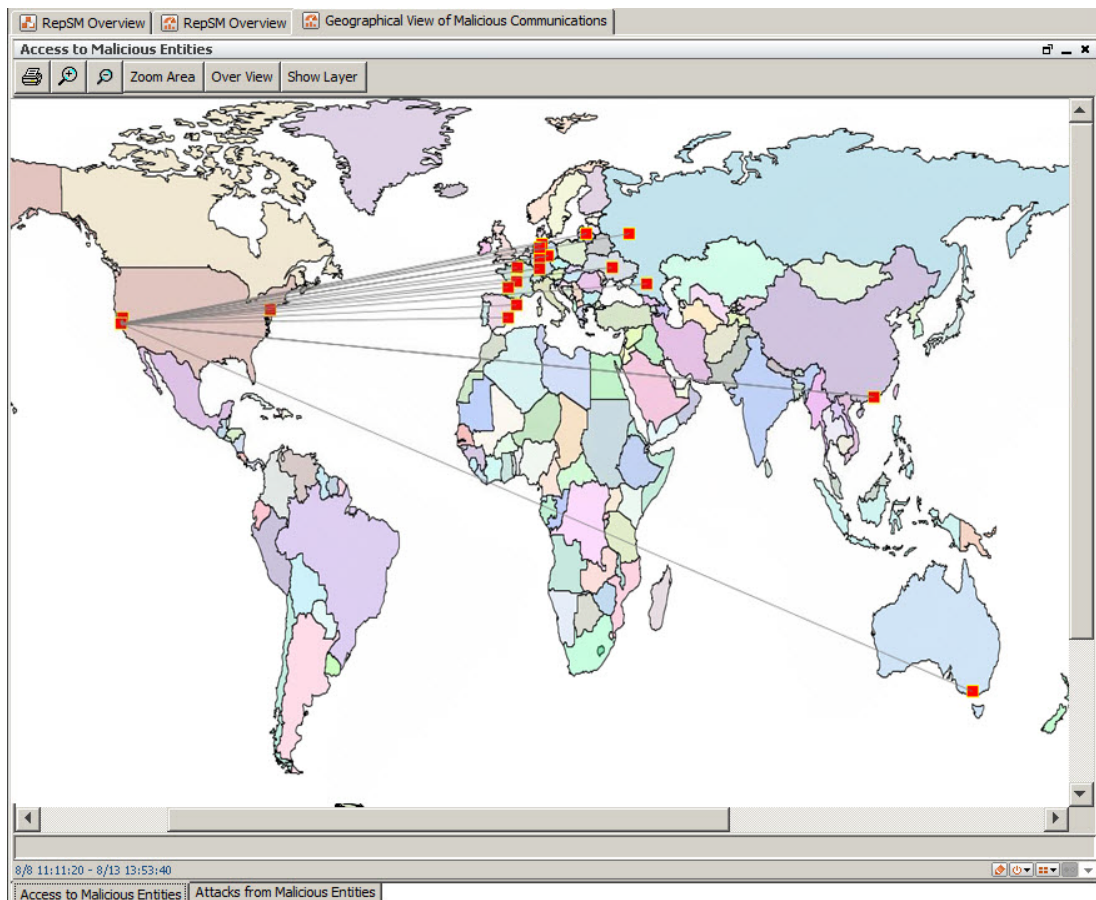
The dashboard provides a high-level, consolidated view of issues based on threat intelligence.



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.



For a complete list of the resources that support this use case, see [“RepSM Overview” on page 111](#).

## 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, see [“RepSM Scenarios” on page 10](#). For information about creating your own scenarios, see [“Creating Custom Scenarios” on page 25](#).

## Configuration

Configure the General Scenarios use case as follows for your environment:

- Optional. If you created any custom scenarios, add them to the Scenarios active list as described in [“Creating Custom Scenarios” on page 25](#).

## Usage

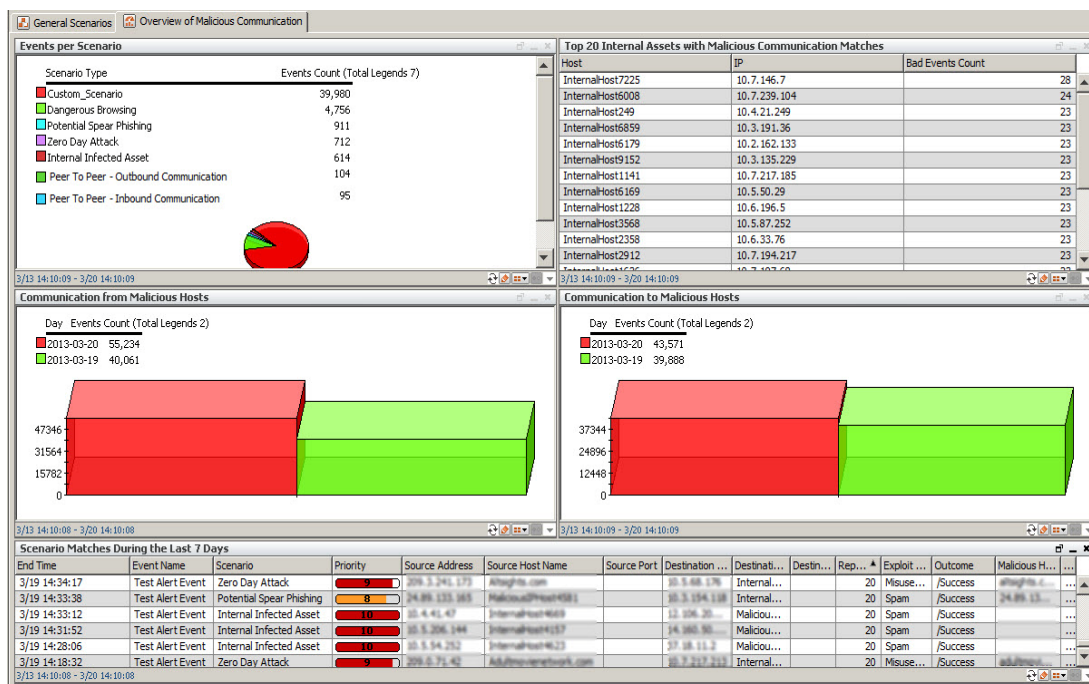
To get started:

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

Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security Monitor 1.5

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

For a complete list of all the resources that support this use case, including the key resources, see [“General Scenarios” on page 95](#).

**Table 3-1** Resources that Support the General Scenarios Use Case

| Resource  | Description  | Type           | URI  |
|---|--|----------------|--|
| <b>Monitor Resources</b>  |  |                |  |
| 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 1.5/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 1.5/General Scenarios/      |
| 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 1.5/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 1.5/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 1.5/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 1.5/General Scenarios/         |

| Resource  | Description  | Type        | URI   |
|---|--|-------------|---|
| 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 1.5/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 1.5/General Scenarios/      |
| <b>Library Resources</b>                                |  |             |   |
| 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 1.5/General Scenarios/ |

## 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 20](#).



This use case opens a case for every detected internal infected asset. For important information about cases, see [“Manage Cases to Ensure Continued Detection” on page 29](#).

## 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 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. This exploit type is the most likely to indicate an infected asset, but 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 20](#).
- 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](#)
 For details, see [“Setting Thresholds for the Reputation Score” on page 23](#).
- Optional. Define your own reputation data by adding entries to the active lists described in [“Including and Excluding Entries from Reputation Data” on page 19](#).

## Usage

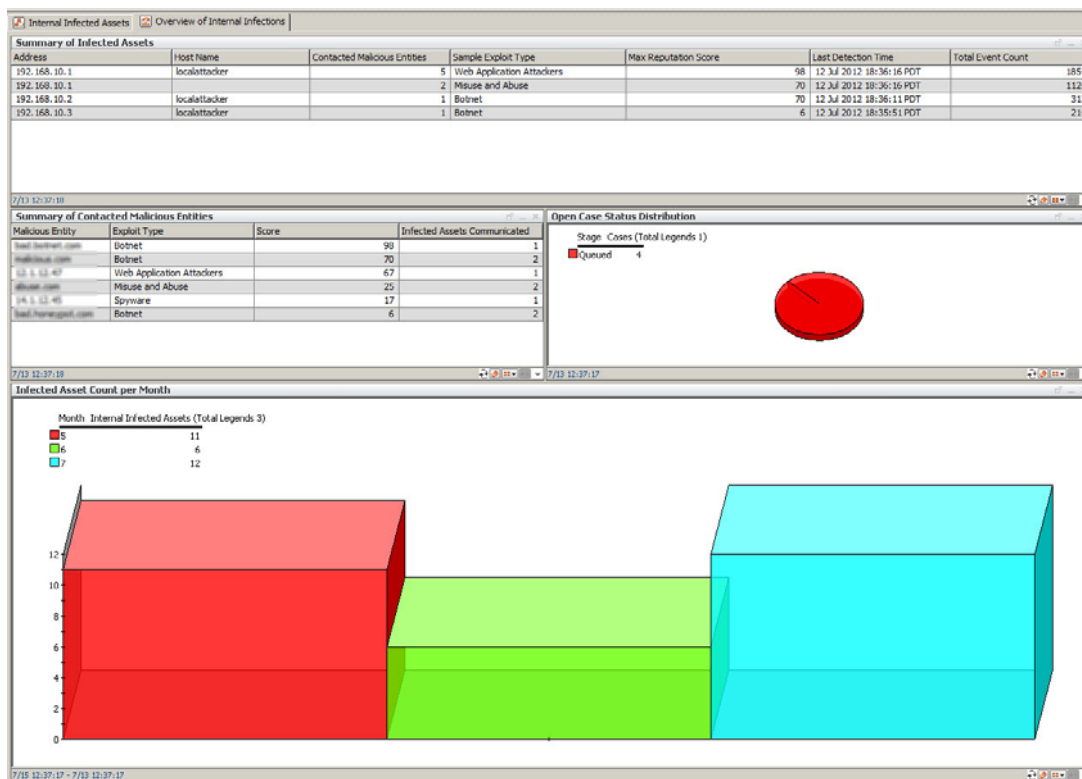
This section describes a likely scenario for investigating internal infected assets and highlights some key features of the use case.

- 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 1.5

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.



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. Right-click an asset and select **Integration Commands > Use TippingPoint to Quarantine** to review your options for quarantining the asset. For more information, see [“Use the TippingPoint Integration Commands” on page 30](#).
  - 9 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 [Step 5](#) and [Step 7](#).
  - 10 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 [“Manage Cases to Ensure Continued Detection” on page 29](#).
  - 11 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.

For a complete list of all the resources that support this use case, including the key resources, see [“Internal Infected Assets” on page 100](#).

**Table 3-2** Resources that Support the Internal Infected Assets Use Case

| Resource  | Description   | Type           | URI   |
|---|---|----------------|---|
| <b>Monitor Resources</b>  |   |                |   |
| 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 1.5/Internal Infected Assets/ |

| Resource  | Description  | Type           | 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.   | Active Channel | /All Active Channels/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Internal Infection Assets/        |
| <b>Library Resources</b>  |  |                |   |
| 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 1.5/Internal Infected Assets/    |



| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| Public-Facing  | This is a solutions asset category.   | Asset Category  | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor          |
| 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 1.5/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 1.5/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 20](#).



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 [“Manage Cases to Ensure Continued Detection” on page 29](#).

## 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 21](#).

- 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. 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 20](#).

- 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 23](#).

- Optional. Define your own reputation data by adding entries to the active lists described in [“Including and Excluding Entries from Reputation Data” on page 19](#).

## Usage

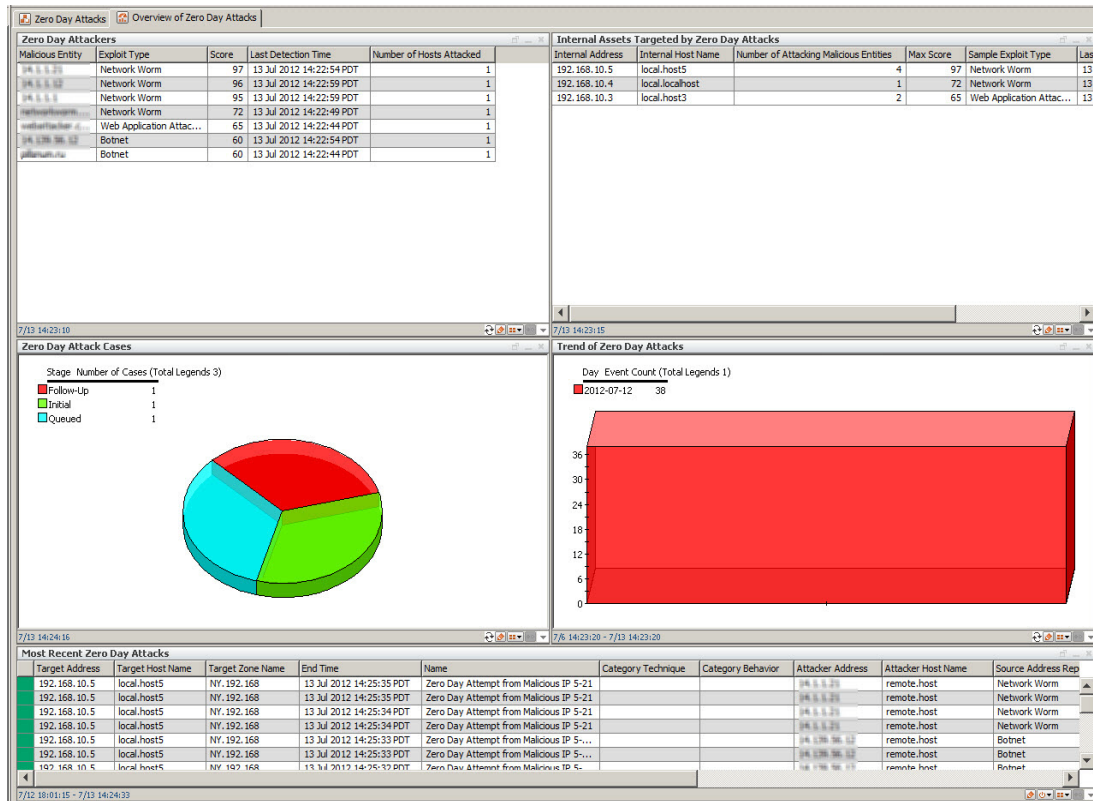
This section describes a likely scenario for investigating zero day attacks and highlights some key features of the use case.

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

Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security Monitor 1.5

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 [“Manage Cases to Ensure Continued Detection” on page 29](#).

- 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.

For a complete list of all the resources explicitly assigned to this use case and any dependant resources, see [“Zero Day Attacks” on page 148](#).

**Table 3-3** Resources that Support the Zero Day Attacks Use Case

| Resource                                  | Description  | Type      | URI  |
|---|--|-----------|--|
| <b>Monitor Resources</b>                  |  |           |  |
| 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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Zero Day Attacks/    |
| <b>Library Resources</b>                  |  |           |  |

| 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 1.5/Zero Day Attacks/ |
| Internal Non Public-Facing                         | This is a solutions asset category.   | Asset Category  | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                   |
| 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 1.5/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 1.5/Configuration/          |

## 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 20](#).

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 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:

- ◆ [Dangerous Browsing Reputation IP Score Threshold](#)
- ◆ [Dangerous Browsing Reputation Domain Score Threshold](#)

For details, see [“Setting Thresholds for the Reputation Score” on page 23](#).

- 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. 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 20](#).

- Optional. Define your own reputation data by adding entries to the active lists described in [“Including and Excluding Entries from Reputation Data” on page 19](#).

## Usage

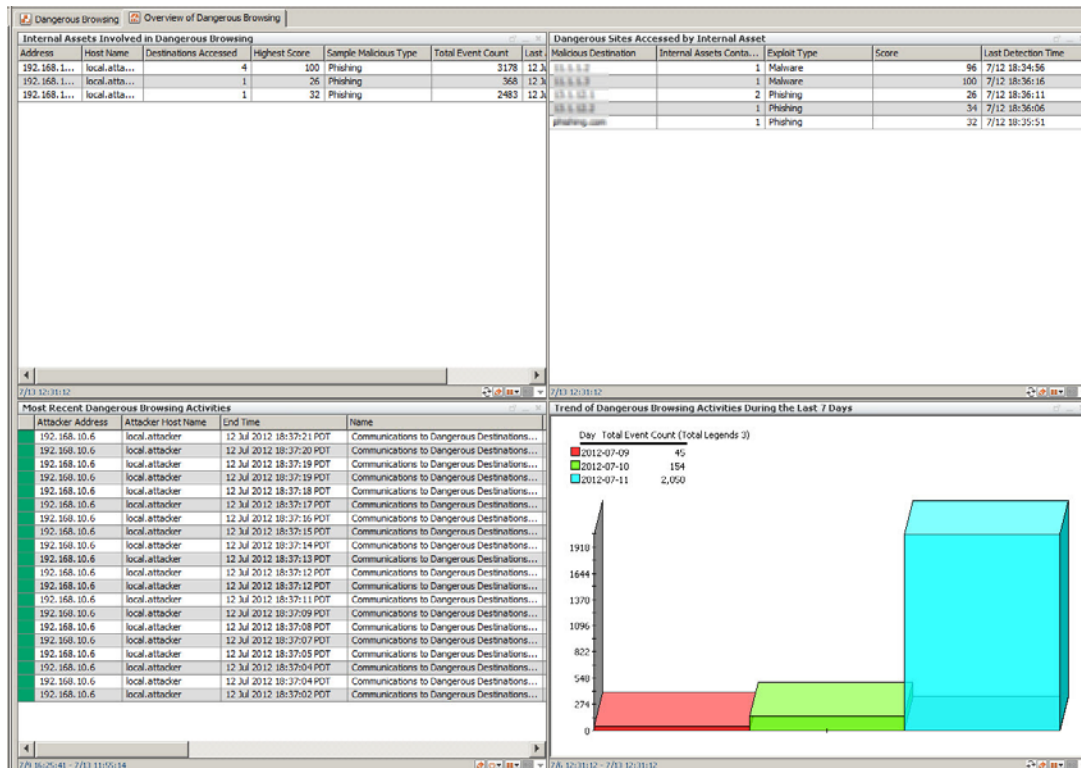
This section describes a likely scenario for investigating users browsing to dangerous web sties and highlights some key features of the use case.

- 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 1.5

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.

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.

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

For a complete list of all the resources explicitly assigned to this use case and any dependant resources, see [“Dangerous Browsing” on page 77](#).

**Table 3-4 Resources that Support the Dangerous Browsing Use Case**

| Resource  | Description  | Type      | URI  |
|---|--|-----------|--|
| <b>Monitor Resources</b>  |  |           |  |
| 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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Dangerous Browsing/    |
| <b>Library Resources</b>  |  |           |  |



| 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 1.5/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 1.5/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 1.5/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.



This use case opens a case for every detected asset found in the reputation data. For important information about cases, see [“Manage Cases to Ensure Continued Detection” on page 29](#).

### 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 Domains for Reputation Monitoring](#) active list. Specify the second-level and third-level domains that represent your organization, for example, `hpe.com` or `hpe.co.uk`.

For details, see [“Configuring Internal Assets Found in Reputation Data” on page 20](#).

- Specify the IP addresses to monitor.

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

The query contains sample conditions for several types of addresses:

- ◆ A network address in Classless Inter-Domain Routing (CIDR) format: `192.168.1.100–192.168.1.150`.
- ◆ A specific network address prefix: `192.168.1`.
- ◆ 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.



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

## Usage

This section highlights some key features of the 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:

Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security Monitor 1.5

Review the resources provided by the use case.

- 2 Open the [Internal Assets and Domains Found in Reputation Data](#) dashboard.

Internal Assets Found in Reputation Data

Internal Assets and Domains Found in Reputation Data

All Internal Domains and Hosts Found

| Domain or Host        | Is a Host Name | Exploit Type     | Score | First Time Found         | Last Time Found          |
|-----------------------|----------------|------------------|-------|--------------------------|--------------------------|
| myorganization.org.us | 0              | Misuse and Abuse | 25    | 3 Jul 2012 12:03:01 PDT  | 13 Jul 2012 12:03:05 PDT |
| myorganization.org    | 0              | Misuse and Abuse | 25    | 3 Jul 2012 12:03:01 PDT  | 13 Jul 2012 12:03:05 PDT |
| etivols.com           | 0              | Botnet           | 75    | 23 May 2012 23:26:00 PDT | 13 Jul 2012 12:03:05 PDT |

7/13 12:34:26

All Internal IP Addresses Found

| Address       | Exploit Type     | Score | First Time Found         | Last Time Found          |
|---------------|------------------|-------|--------------------------|--------------------------|
| 192.168.1.1   | Misuse and Abuse | 9     | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.10  | Spyware          | 15    | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.100 | Botnet           | 94    | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.101 | Malware          | 100   | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.102 | Phishing         | 34    | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.103 | Phishing         | 26    | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |
| 192.168.1.104 | Botnet           | 98    | 23 May 2012 23:00:07 PDT | 13 Jul 2012 12:00:05 PDT |

7/13 12:34:26

- 3 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.
- 4 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:

Cases/Shared/All Cases/ArcSight Solutions/RepSM/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 [“Manage Cases to Ensure Continued Detection” on page 29](#).

- 5 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.



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, the asset might reappear in the active lists. To remove the asset more permanently, contact Customer Support.

## 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.

For a complete list of all the resources that support this use case, including the key resources, see [“Internal Assets Found in Reputation Data” on page 98](#).

**Table 3-5** Resources that Support the Internal Assets Found in Reputation Data Use Case

| Resource   | Description  | Type        | URI  |
|--|--|-------------|--|
| <b>Monitor Resources</b>                             |  |             |  |
| 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 1.5/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 1.5/Internal Assets Found in Reputation Data/      |
| <b>Library Resources</b>                             |  |             |  |
| 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 hpe.com or hpe.co.uk. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/ |

| Resource  | Description  | Type        | 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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/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 resources. By enriching those resources with global threat intelligence, security analysts can focus on key events involving known malicious entities.

### Configuration

No configuration is required for this use case.

### Usage

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 [Table 3-6](#) 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](#)
- [Source Domain Reputation Exploit Type](#)

This is just one example; for a description and the location of these and other variables, see [Table 3-6](#).

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

### 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.

For a complete list of all the resources that support this use case, including the key resources, see [“Event Enrichment with Reputation Data” on page 90](#).

**Table 3-6** Resources that Support the Event Enrichment with Reputation Data Use Case

| Resource                                    | Description  | Type            | URI   |
|---|--|-----------------|---|
| <b>Library Resources</b>                    |  |                 |   |
| 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 1.5/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 1.5/Event Enrichment with Reputation Data/ |

| Resource                               | Description   | Type            | URI   |
|--|---|-----------------|---|
| 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 1.5/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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Event Enrichment with Reputation Data/ |
| 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 1.5/Event Enrichment with Reputation Data/ |

| Resource  | Description   | Type               | URI   |
|---|---|--------------------|---|
| Request URL<br>Domain<br>Reputation<br>Exploit Type | This variable returns the exploit type of a domain from a URL request based on the reputation domain data.                                | Global<br>Variable | /All Fields/ArcSight<br>Solutions/Reputation<br>Security Monitor 1.5/Event<br>Enrichment with Reputation<br>Data/   |
| Destination<br>Reputation<br>Domain                 | This variable returns the reputation domain related to a malicious target (or destination) host name based on the reputation domain data. | Global<br>Variable | /All Fields/ArcSight<br>Solutions/Reputation<br>Security Monitor 1.5/Event<br>Enrichment with Reputation<br>Data/   |
| Request URL<br>Enrichment                           | This field set contains fields with reputation information (based on the request URL) for event enrichment purposes.                      | Field Set          | /All Field Sets/ArcSight<br>Solutions/Reputation<br>Security Monitor 1.5/   |
| Reputation IP<br>Enrichment                         | This field set contains fields with reputation IP information for event enrichment purposes.  | Field Set          | /All Field Sets/ArcSight<br>Solutions/Reputation<br>Security Monitor 1.5/   |
| Reputation<br>Domain<br>Enrichment                  | This field set contains fields with reputation domain information for event enrichment purposes.  | Field Set          | /All Field Sets/ArcSight<br>Solutions/Reputation<br>Security Monitor 1.5/   |
| Events to<br>Malicious<br>Targets                   | This filter identifies events whose targets are found in the reputation database.   | Filter             | /All Filters/ArcSight<br>Solutions/Reputation<br>Security Monitor<br>1.5/Events Enrichment with<br>Reputation Data/ |
| Events from<br>Malicious<br>Sources                 | This filter identifies events whose attackers are found in the reputation database.   | Filter             | /All Filters/ArcSight<br>Solutions/Reputation<br>Security Monitor<br>1.5/Events Enrichment with<br>Reputation Data/ |
| Events with<br>Requests to<br>Malicious<br>Hosts    | This filter identifies events with requests to hosts found in the reputation database.  | Filter             | /All Filters/ArcSight<br>Solutions/Reputation<br>Security Monitor<br>1.5/Events Enrichment with<br>Reputation Data/ |
| RepSM<br>Relevant<br>Events                         | This filter identifies events that contains information related to reputation data (for example, host address or request URL).            | Filter             | /All Filters/ArcSight<br>Solutions/Reputation<br>Security Monitor<br>1.5/Events Enrichment with<br>Reputation Data/ |



# RepSM Package Health Status

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

For an explanation of RepSM service messages, see [Appendix C, RepSM Service Messages](#), on page 75.

## Configuration

No special configuration is required for this use case.

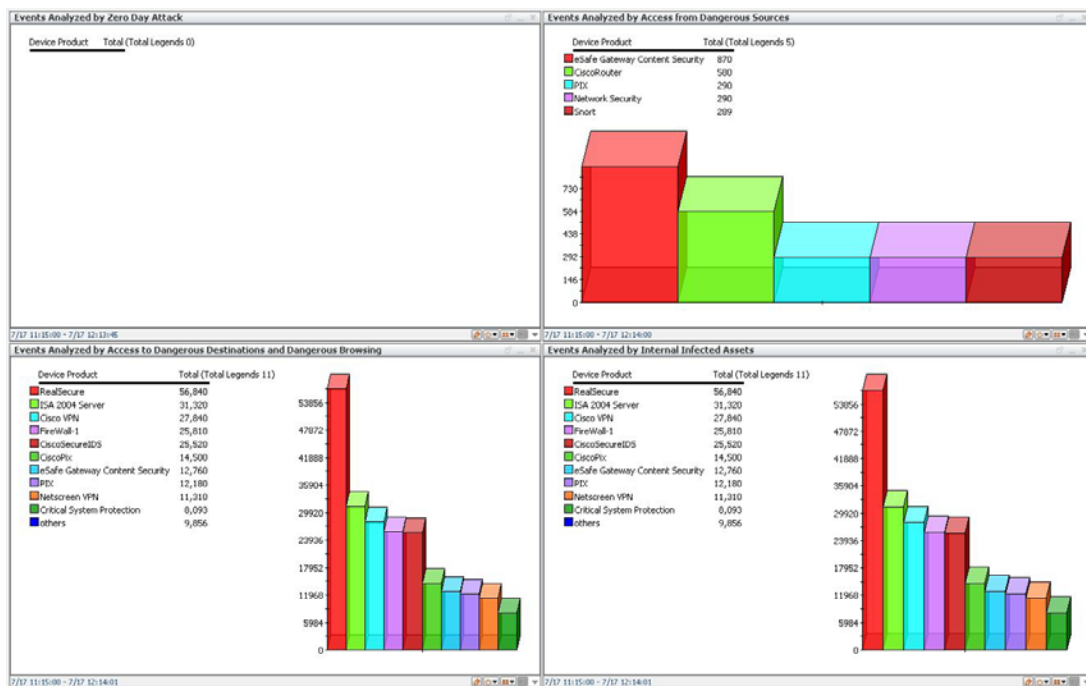
## Usage

This section highlights some key features of the use case.

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

Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security Monitor 1.5

- 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 [Appendix A, Troubleshooting, on page 63](#).

- 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, rule error logs, and trend query failures.

This dashboard also displays messages about RepSM service activation and data retrieval. For an explanation of those messages, see [Appendix C, RepSM Service Messages, on page 75](#).

- 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.

For a complete list of all the resources that support this use case, including the key resources, see [“RepSM Package Health Status” on page 124](#).

**Table 3-7** Resources that Support the RepSM Package Health Status Use Case

| Resource                           | Description   | Type      | URI   |
|------------------------------------|---|-----------|---|
| <b>Monitor Resources</b>           |   |           |   |
| 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 1.5/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 1.5/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 1.5/RepSM Package Health Status/ |

---

| Resource                    | Description  | Type      | URI   |
|-----------------------------|--|-----------|---|
| RepSM<br>Resource<br>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. | Dashboard | /All Dashboards/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/ |

---

## 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.

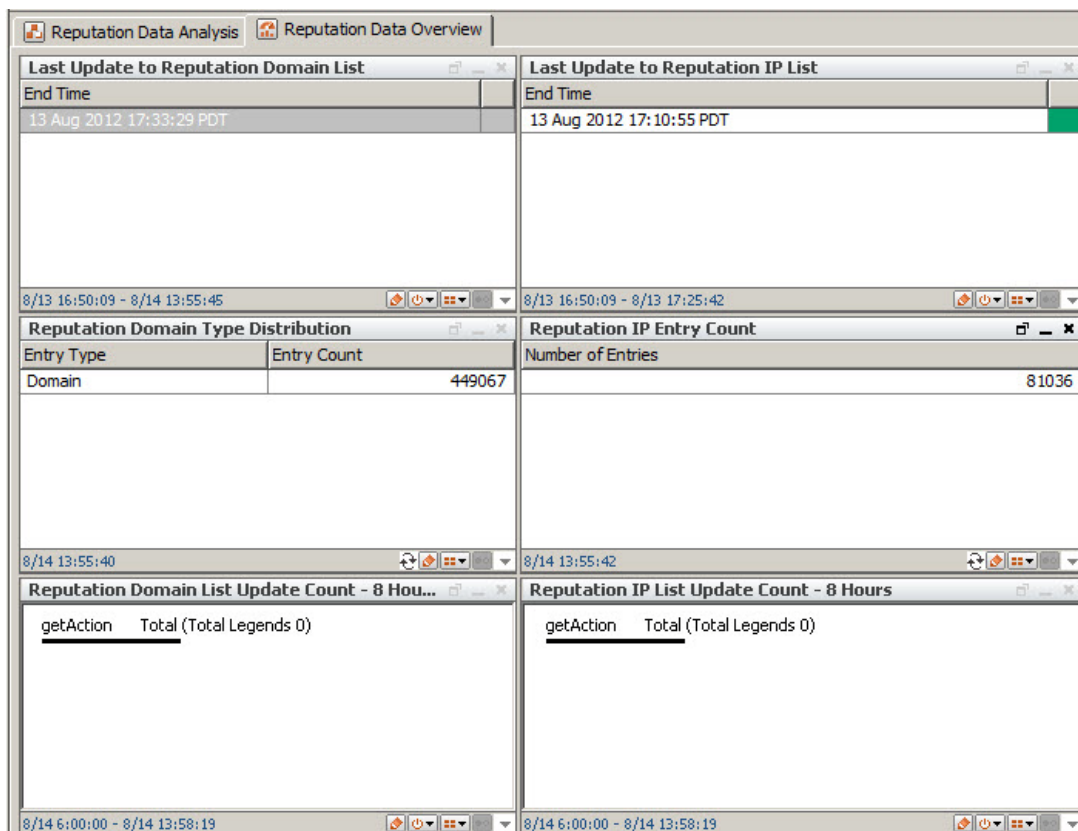
### Configuration

No special configuration is required for this use case.

### Usage

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:  
Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation Security Monitor 1.5
- 2 Open the [Reputation Data Overview](#) dashboard to see when the reputation data was last updated by the Model Import Connector for RepSM.



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.

For a complete list of all the resources explicitly assigned to this use case and any dependant resources, see [“Reputation Data Analysis” on page 143](#).

**Table 3-8** Resources that Support the Reputation Data Analysis Use Case

| Resource                            | Description  | Type         | URI   |
|-------------------------------------|--|--------------|---|
| <b>Monitor Resources</b>            |  |              |   |
| 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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Reputation Data Analysis/ |

| Resource   | Description   | Type   | URI   |
|--|---|--------|---|
| 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 1.5/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. | Report | /All Reports/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/Reputation Data Analysis/ |

## Appendix A

# Troubleshooting

---

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

**Table A-1** RepSM Troubleshooting (Sheet 1 of 3)

| Problem   | Solution   |
|---|--|
| The installation of the RepSM content package fails with the following error:<br><br>Install Failed: ActiveList capacity cannot be greater than <i>nnnnnn</i><br><br><i>nnnnnn</i> will vary depending on whether you are installing RepSM on ArcSight ESM or ArcSight Express. | Increase the active list maximum capacity, as described in <a href="#">“Configuring the Active List Capacity (Required)” on page 14</a> .    |
| On ArcSight ESM, the Manager slows down or stops responding during the import of reputation data from the RepSM service.  | Increase the ArcSight Manager Java heap memory size to at least 4 GB, as described in the ArcSight ESM Installation and Configuration Guide. |

**Table A-1** RepSM Troubleshooting (Sheet 2 of 3)

| Problem   | Solution   |
|---|--|
| The RepSM use cases do not appear to be working; their dashboards and reports do not display any events or reputation data.   | <p>In the following order:</p> <ul style="list-style-type: none"> <li>• Make sure the Model Import Connector for RepSM is running.</li> <li>• Make sure the Model Import Connector for RepSM is not out of memory. Look for an <code>OutOfMemoryError</code> message in the <code>\$ARCSIGHT_HOME\current\logs\agent.log</code>. 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 Configuration Guide.</li> <li>• Make sure the <b>Model Import User</b> is configured in the ArcSight Manager, as described in the Model Import Connector for RepSM Configuration Guide. Otherwise, the Manager cannot accept reputation data from the RepSM service.</li> <li>• Make sure the ArcSight Manager is collecting events from the devices described in <a href="#">“Supported Devices” on page 12</a>.</li> <li>• Make sure the RepSM rules are deployed, as described in <a href="#">“Deploying Rules” on page 22</a>.</li> <li>• Make sure the use case is configured properly. Several use cases require asset categorization or other configuration to capture events. For configuration details, see <a href="#">“Configuring the RepSM Content” on page 17</a> and <a href="#">Chapter 3, Using RepSM Content, on page 27</a>.</li> <li>• Make sure inbound events are being sent to ArcSight Manager. Check the Inbound Events active channel.</li> <li>• Make sure outbound events are being sent to ArcSight Manager. Check the Outbound Events active channel.</li> <li>• Make sure the event source connector and ArcSight Manager are synchronized; the <i>Manager Receipt Time</i> should be no more than a few seconds later than the event <i>End Time</i>. Use the Inbound Events or Outbound Events active channel to open an event in the Event Inspector and compare these times.</li> </ul> |
| <p>The number of reputation data entries imported into the ArcSight Manager seems very low.</p> <p>There might also be reputation data archive files that have a file extension of <code>.xml.bad</code> in <code>ARCSIGHT_HOME\archive\webservices</code>.</p> | <p>Make sure the following Model Import Connector for RepSM property is set in the <code>agent.properties</code> file located at <code>ARCSIGHT_HOME\current\user\agent</code>:</p> <pre>buildmodeldelay=60000 (one minute expressed in milliseconds)</pre> <p>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 Configuration Guide.</p>  |



**Table A-1** RepSM Troubleshooting (Sheet 3 of 3)

| Problem   | Solution   |
|---|--|
| The RepSM use case dashboards do not show any <i>recent</i> activity; the data seems stale.   | <p>Check the <a href="#">Reputation Data Overview</a> 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 service or the Model Import Connector for RepSM. For example, the service might have expired or the connector might need to be restarted.</p> <p>To check the status of either component, open the RepSM Package Health Status use case and review the messages in the <a href="#">RepSM Resource Health</a> dashboard. For an explanation of the service messages, see <a href="#">Appendix C, RepSM Service Messages, on page 75</a>.</p> <p>If the messages do not reveal any obvious issues, search the connector log at <code>\$ARCSIGHT_HOME\current\logs\agent.log</code> for network error messages, such as:</p> <ul style="list-style-type: none"> <li>• connection timeout</li> <li>• host cannot be reached</li> </ul> <p>and address those network issues.</p> <p>If there are no obvious network issues, look for an <code>OutOfMemoryError</code> message in the <code>\$ARCSIGHT_HOME\current\logs\agent.log</code>. 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 Configuration Guide.</p> <p>While less likely, the problem might be caused by a planned outage of the RepSM service. Check the RepSM group on Protect 724 to see if there is a planned outage:</p> <p><a href="https://protect724.arcsight.com/groups/repasm">https://protect724.arcsight.com/groups/repasm</a></p> <p>If you cannot determine cause of the problem, contact Customer Support.</p> |
| The reputation data includes an entry for an IP address, host name, or domain name that is <b>not</b> malicious.                                | <p>Consider adding an entry to the Exceptions active lists, as described in <a href="#">“Including and Excluding Entries from Reputation Data” on page 19</a>.</p> <p>To remove an entry more permanently from the reputation data, gather the following information and contact Customer Support.</p> <ul style="list-style-type: none"> <li>• The IP address, host name, or domain name to be removed.</li> <li>• Any relevant event details (depending on the source of the event), such as the request URL, source port, destination port, and matching signature.</li> </ul>  |
| On ArcSight ESM, some dashboards display <i>numerical</i> exploit types. (Exploit types should be text, such as Botnet, Spam, Spyware, or P2P.) | Increase the ArcSight Manager Java heap memory size to at least 4 GB, as described in the ArcSight ESM Installation and Configuration Guide, and restart the Manager.  |



# Upgrading and Uninstalling RepSM

---

This appendix provides instructions on how to upgrade and uninstall RepSM.



In this section, RepSM 1.5 is either RepSM 1.5 or RepSM 1.51.

You must upgrade RepSM 1.0 or 1.01 to **RepSM 1.5** before you upgrade to RepSM 1.52. Refer to the *HPE Reputation Security Monitor 1.5 Solution Guide* for details.

## Upgrade from RepSM 1.5

RepSM 1.5 must be uninstalled before you install RepSM 1.52. Perform the following tasks in the order shown:

- 1 [“Stop the Model Import Connector for RepSM” on page 67.](#)
- 2 [“Identify Customized Resources” on page 68.](#)
- 3 [“Back Up the Reputation Data Active Lists” on page 68.](#)
- 4 [“Back Up RepSM 1.5” on page 70.](#)
- 5 [“Uninstall RepSM 1.5” on page 71.](#)
- 6 [“Install RepSM 1.52” on page 72.](#)
- 7 [“Import the Backed Up Active Lists” on page 72.](#)
- 8 [“Customize the RepSM 1.52 Resources” on page 72.](#)
- 9 [“Install the Model Import Connector for RepSM” on page 73.](#)
- 10 [“Start the Model Import Connector for RepSM” on page 73.](#)

[Step 2](#), [Step 4](#), and [Step 8](#) are necessary only if you want to preserve customized RepSM 1.5 resources.

Assets that were categorized with the RepSM 1.5 categories do not need to be recategorized in RepSM 1.52.

## Stop the Model Import Connector for RepSM

Stop the Model Import Connector for RepSM, as described in the Model Import Connector for RepSM Configuration Guide.

## Identify Customized Resources

You can identify customized RepSM 1.5 resources by generating a list of resources that have changed since the solution packages were last exported. You can then use these resources as a reference for applying the same customizations to the RepSM 1.52 resources.



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

### To identify changed resources:

- 1 Log into the ArcSight Console with an account that has administrative privileges.
- 2 In the **Packages** tab of the Navigator panel, navigate to the ArcSight Solutions group.
- 3 Right-click the Reputation Security Monitor 1.5 package (📁) and select **Compare Archive with Current Package Contents**.

In the Viewer panel, a list of resources associated with the package are displayed. In the right column called *Change Since Archive*, any changes with the resource since the last export are displayed, either Added, Modified, or Removed.

To sort the list and display the changed resources together, click the *Change Since Archive* column.

| Type        | Parent URI   | Resource                                  | Change Since Archive |
|-------------|--|---|----------------------|
| Active List | /All Active Lists/ArcSight Solutions/Reputation S... | PC Reputation Domains                     |                      |
| Active List | /All Active Lists/ArcSight Solutions/Reputation S... | PC Reputation IPs                         |                      |
| Active List | /All Active Lists/ArcSight Solutions/Reputation S... | Top Reputation Domains                    | Modified             |
| Active List | /All Active Lists/ArcSight Solutions/Reputation S... | Top Reputation IPs                        | Modified             |
| Case        | /All Cases/All Cases/ArcSight Solutions/Reputati...  | Internal Infection: Outbound Request...   |                      |
| Case        | /All Cases/All Cases/ArcSight Solutions/Reputati...  | Internal Infection: Outbound Traffic t... |                      |
| Case        | /All Cases/All Cases/ArcSight Solutions/Reputati...  | Internal Infection: Outbound Traffic t... |                      |
| Case        | /All Cases/All Cases/ArcSight Solutions/Reputati...  | Internal Infection: Outbound Traffic t... |                      |
| Case        | /All Cases/All Cases/ArcSight Solutions/Reputati...  | Internal Infection: Outbound Traffic t... |                      |

- 4 Optional—For future reference, you can copy and paste the cells from this table into a spreadsheet.

## Back Up the Reputation Data Active Lists

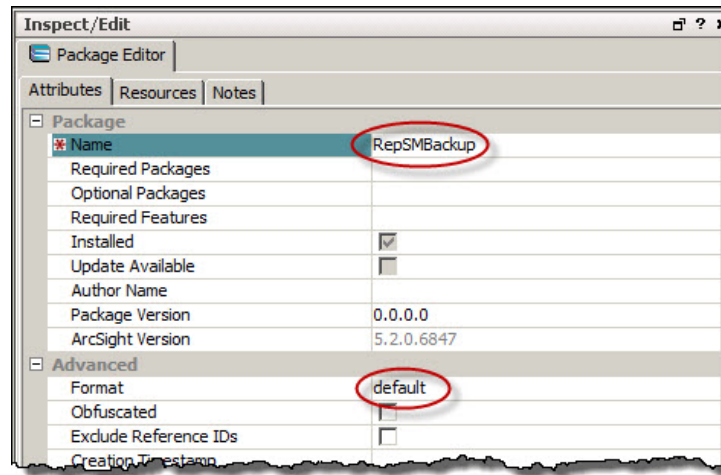
This step is required if you want to preserve the reputation data in the active lists in the /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data folder; otherwise, the RepSM 1.52 active lists will be empty.

Use the following procedure to back up the data in the active lists, so you can import the data into RepSM 1.52.

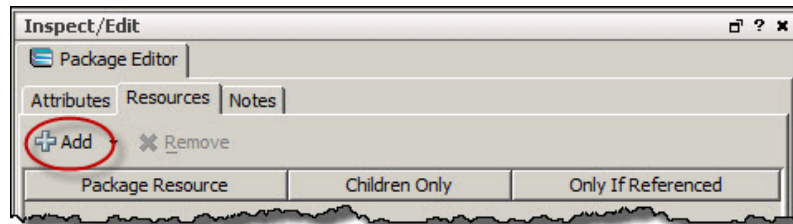
- 1 Log into the ArcSight Console.
- 2 In the Navigator panel, on the Packages tab, right-click Shared/All Packages/Public and select **New Package**.

The Package Editor opens in the Inspect/Edit panel.

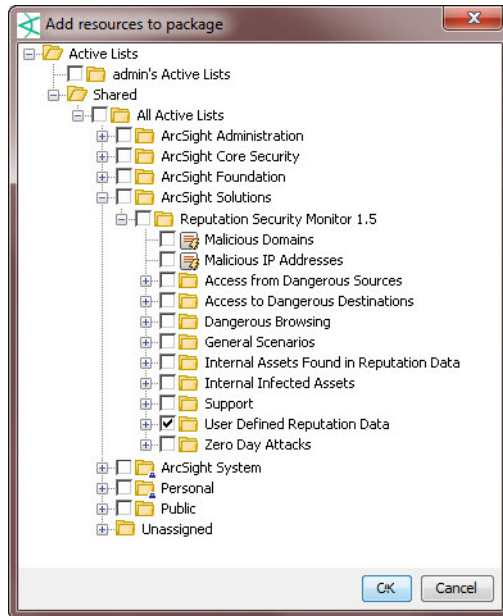
- 3 On the **Attributes** tab, in the **Name** field, type a name for the package, for example, RepSMBBackup, and make sure the **Format** field is set to default:



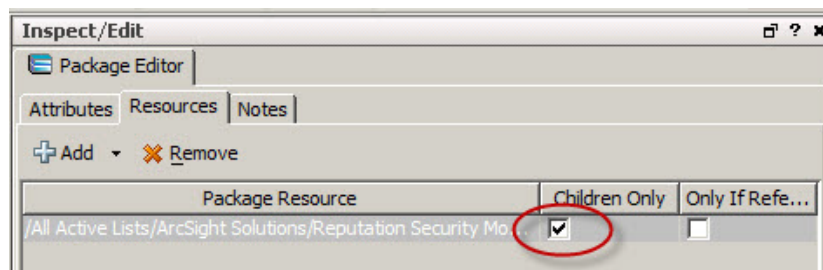
- 4 On the **Resources** tab, click **Add**, then select **Lists | Active Lists**.



- 5 Check the box next to Active Lists/Shared/All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data and click **OK**.



- 6 Check the **Children Only** boxes. Otherwise, when you import the backup package later, the RepSM group name reverts to 1.5 instead of 1.52. The Resources tab looks like this:



- 7 Click **OK** to save the package.
- 8 In the Navigator panel, on the Packages tab, expand the Public folder, right-click the newly created backup package, select **Export Package to Bundle**, and save the .arb file to the local disk.
- 9 Right-click the backup package and select **Uninstall Package**.

## Back Up RepSM 1.5

HPE recommends that you keep a backup of the current state before making content changes or installing and uninstalling solution packages. Before backing up a solution, you can obtain a list of changed resources. You can then back up only those resources that have been modified or added. For detailed instructions, see ["Identify Customized Resources" on page 68](#).

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

**To back up a solution package:**

- 1 Log into the ArcSight Console with an account that has administrative privileges.
- 2 In the **Packages** tab of the Navigator panel, navigate to All Packages/ArcSight Solutions.
- 3 Right-click the Reputation Security Monitor 1.5 package (📁) and select **Export Package to Bundle**.

The Package Bundle Export dialog displays.

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

The Progress tab of the Export Packages dialog displays the progress of the export.

- 5 When the export is complete, click **OK**.


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

## Uninstall RepSM 1.5

Before uninstalling the RepSM content package, back up all the packages (📁) for all the solutions currently installed. For example, if the RepSM content and the CIP for SOX solution are both installed on the same ArcSight ESM, export the package for each solution before uninstalling either solution. Back up the CIP for SOX package into a package bundle (`.arb`) file and then back up the RepSM content package into a different package bundle (`.arb`) file before uninstalling either solution.

**To uninstall the content package:**

- 1 Log into the ArcSight Console with an account that has administrative privileges.  
  
Do not uninstall RepSM as the `systemuser`. Doing so uninstalls resources that are intentionally locked.
- 2 Delete any snapshots that were generated by RepSM:
  - a In the Navigator panel Resources tab, select **Pattern Discovery** from the drop-down menu.
  - b Click the **Snapshots** tab, navigate to All Snapshots/ArcSight Solutions/Reputation Security Monitor 1.5 and expand the group.

- c Press the **Ctrl** key and click each snapshot, until all the snapshots are highlighted.
    - d Right-click the snapshots, select **Delete Snapshot**, and agree to the delete confirmation prompt.
  - 3 Delete any patterns that were generated by RepSM:
    - a In the Navigator panel Resources tab, click the **Patterns** tab, navigate to All Patterns/Arcsight Solutions/Reputation Security Monitor 1.5 and expand the group.
    - b Press the **Ctrl** key and click each pattern group, until all the groups are highlighted.
    - c Right-click the groups, select **Delete Group**, and agree to the delete confirmation prompts.
  - 4 Click the **Packages** tab in the Navigator panel.
  - 5 Navigate to ArcSight Solutions, right-click the Reputation Security Monitor 1.5 package () , and select **Uninstall Package**.
  - 6 In the Uninstall Packages dialog, click **OK**. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.

If a message indicates a conflict about locked resources, select the **Skip** option in the **Resolution Options** area and click **OK**.

If a message indicates a conflict about changed package content, select the **Continue without saving changes** option and click **OK**.
  - 7 When the uninstall is finished, review the summary and click **OK**.
  - 8 Right-click the Reputation Security Monitor 1.5 package and select **Delete Package**.

## Install RepSM 1.52

Import and install the RepSM 1.52 package, as described in [“Installing the RepSM Content” on page 14](#).

## Import the Backed Up Active Lists

Skip this section if you chose not to back up the active lists from the previous version of RepSM.

- 1 Import and install the backup .arb file that you created in [Step 8 on page 70](#) to restore the data from the old active lists to the new active lists.
- 2 After successfully importing the backup .arb file, right-click the active lists in the Navigator panel Resources tab and select **Show Entries** to display the restored entries.

## Customize the RepSM 1.52 Resources

For the resources that you identified in [“Identify Customized Resources” on page 68](#), use the RepSM 1.5 resources as a reference to make the same customizations to the RepSM 1.52 resources.



## **Install the Model Import Connector for RepSM**

Install the Model Import Connector for RepSM, as described in the Model Import Connector for RepSM Configuration Guide. See the Reputation Security Monitor Release Notes for the required version of the connector.

## **Start the Model Import Connector for RepSM**

Start the Model Import Connector for RepSM, as described in the Model Import Connector for RepSM Configuration Guide.



## Appendix C

# RepSM Service Messages

This appendix explains some of the more important RepSM service messages that appear in the [RepSM Resource Health](#) dashboard of the RepSM Package Health Status use case.

## Service Activation Messages

The following messages are issued during the activation of the RepSM service.

| Message   | Explanation   | User Action   |
|---|---|---|
| 1: Invalid key  | The activation of the RepSM service failed due to an invalid activation key.                                    | Specify a valid activation key by reconfiguring the Model Import Connector for RepSM. The activation key is provided by HPE. For more information, see the Model Import Connector for RepSM Configuration Guide.<br><br>If the activation continues to fail, contact HPE ArcSight Customer Support. |
| 3: Trial period expired on<br><i>YYYY-MM-DDThh:mm:ssZ</i> | The activation of the RepSM service failed because the trial license expired on the date shown in the message.  | Contact your HPE ArcSight sales representative to obtain a new license.   |
| 4: Key expired on<br><i>YYYY-MM-DDThh:mm:ssZ</i>          | The activation of the RepSM service failed because the activation key expired on the date shown in the message. | Contact your HPE ArcSight sales representative to obtain a new activation key.  |
| 5: Service terminated on<br><i>YYYY-MM-DDThh:mm:ssZ</i>   | The activation of the RepSM service failed because the service was terminated on the date shown in the message. | If your organization requested the termination, no action is required.<br><br>If your organization did not request the termination, contact HPE ArcSight Customer Support.  |

## Data Retrieval Messages

The following messages are issued by the Model Import Connector for RepSM when it attempts to retrieve reputation data from the RepSM service.

| Message   | Explanation   | User Action  |
|---|---|--|
| 0: OK   | The request to retrieve data from the RepSM service was successful.   | No action is required.   |
| 1: Invalid service key                              | The request to retrieve data from the RepSM service failed because the service key cannot be found in the database, or the service key is invalid.  | Contact HP ArcSight Customer Support.  |
| 3: Database not found with requested version        | An incremental update of data from the RepSM service was not available, so a full import will be performed. The RepSM active lists will be repopulated with new entries from the full import. | No action is required.   |
| 4: Service terminated on <i>DD-MM-YYYYThh:mm:ss</i> | The request to retrieve data from the RepSM service failed because the license was terminated on the date shown in the message.   | If your organization requested the termination, no action is required.<br>If your organization did not request the termination, contact HPE ArcSight Customer Support. |
| 5: Service will expire in <i>nn</i> days            | The request to retrieve data from the RepSM service was successful, but the service will expire soon. (This message will be implemented in a future release.)                                 | No action is required.   |

## Appendix D

# RepSM Resource Reference

This appendix lists all of the resources explicitly assigned to each RepSM use case, and any dependent resources. The resources are organized by use case, as follows:

[“Dangerous Browsing” on page 77](#)  
[“Event Enrichment with Reputation Data” on page 90](#)  
[“General Scenarios” on page 95](#)  
[“Internal Assets Found in Reputation Data” on page 98](#)  
[“Internal Infected Assets” on page 100](#)  
[“Reputation Data Analysis” on page 143](#)  
[“RepSM Overview” on page 111](#)  
[“RepSM Package Health Status” on page 124](#)  
[“Zero Day Attacks” on page 148](#)

For information about the key resources for each use case, see the “Key Resources” sections in [Chapter 3, Using RepSM Content, on page 27](#). Key resources are those that you use during an investigation or that might require configuration.

## Dangerous Browsing

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-1** Resources that Support the Dangerous Browsing Use Case

| Resource                       | Description  | Type      | URI  |
|--------------------------------|--|-----------|--|
| <b>Monitor Resources</b>       |  |           |  |
| 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 1.5/Dangerous Browsing/ |

| Resource   | Description  | Type         | URI   |
|--|--|--------------|---|
| 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. | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/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 1.5/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 1.5/Dangerous Browsing/             |
| <b>Library - Correlation Resources</b>                                     |  |              |   |
| 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.  | Rule         | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| 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.  | Rule         | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |

| Resource  | Description   | Type        | URI  |
|---|---|-------------|--|
| 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.   | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/        |
| <b>Library Resources</b>  |   |             |  |
| Malicious IP Addresses  | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.  | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                  |
| Additional Malicious Domains  | This active list enables user to define reputation domain names.  | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| Exceptions - IPs  | This active list enable the user to define entries which will NOT be considered bad.  | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| 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 1.5/Internal Infected Assets/         |
| 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 1.5/Access to Dangerous Destinations/ |
| Exceptions - Domains  | This active list enable the user to define entries which will NOT be considered bad.  | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| 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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |

| Resource   | Description   | Type            | 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. | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/    |
| Additional Malicious IP Addresses                            | This active list enables user to define reputation IP addresses.  | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/        |
| Malicious Domains  | This active list stores up to 1,500,000 reputation domain names from the RepDV database.  | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                     |
| Support RepSM Advanced Content                               | This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.   | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                             |
| Protected  | This is a site asset category.  | Asset Category  | /All Asset Categories/Site Asset Categories/Address Spaces  |
| Public-Facing  | This is a solutions asset category.   | Asset Category  | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                                      |
| Most Recent Dangerous Browsing Activities                    | This data monitor shows the last 20 dangerous browsing activities from non public-facing internal assets.   | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/                 |
| solnGetTargetReputationDomainLevel4ListEntry                 | This variable returns the entry in the reputation domain list corresponding to the target domain level 4.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetURLIP   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetRequestURLDomainLevel2                                | This variable returns the two rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |



| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGenericHighScoreThreshold                                  | This global variable defines the generic threshold for high reputation scores.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |
| solnGetDestinationScore  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetDestinationExceptionHostNameListEntry                   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetDestinationAdditionalDataDomainEntry                    | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetDestinationAdditionalDataDomainLevel2ListEntry          | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetReputationDomainLevel3ListEntry                   | This variable returns the entry in the reputation domain list corresponding to the target domain level 3.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainEntry                             | This variable returns the entry of a target in the reputation domain list used for real time correlation.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLDomainLevel2ListEntry                         | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationIPListEntry                             | This variable returns the target address entry in the reputation IP database.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetURLDomain   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetLowerTargetHostName                           | This variable returns the target host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainLevel2ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetDomainLevel3                            | This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.            | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| 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 1.5/Configuration/                             |
| solnGetRequestURLDomain                              | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnCheckDestinationIsInExceptionsDomainList         | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetTargetDomainLevel2                            | This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetBaseRequestURLAdditionalDataDomainEntry       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| 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 1.5/Configuration/                             |
| solnGetRequestURLDomainExploitType                   | This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetTargetDomainExploitType                       | This variable returns the exploit type of a target in the reputation domain list used for real time correlation.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetURLScore                                      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetDestinationExceptionDomainLevel3ListEntry      | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetDestinationIP                                  | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetURLExploitType                                 | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetTargetDomainLevel4                             | This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainEntry            | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLAdditionalDataDomainLevel4ListEntry  | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationAdditionalDataDomainLevel4ListEntry | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationExceptionDomainLevel4ListEntry      | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetLowerDestinationHostName                       | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainLevel4ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainLevel2ListEntry          | This variable returns the entry in the reputation domain list corresponding to the target domain level 2.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetDestinationAdditionalDataHostNameListEntry                  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetRequestURLDomainLevel1                                      | This variable returns the right most subdomain of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainLevel4                                      | This variable returns the 4 right most subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationDomain   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetTargetReputationHostNameListEntry                           | This variable returns the entry of a target host name in the reputation domain list used for real time correlation.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetDestinationExploitType                                      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetDestinationExceptionDomainLevel2ListEntry                   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnNullAddresses  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationExceptionIPLISTEntry                             | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |
| solnGetRequestURLDomainLevel3ListEntry                             | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetRequestURLDomainLevel1ListEntry                    | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetRequestURLReputationDomainEntry                    | This variable returns the entry of a request URL in the reputation domain list used for real time correlation.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLAdditionalDataDomainLevel3ListEntry      | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetRequestURLDomainLevel3                             | This variable returns the three rightmost subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationAdditionalDataDomainLevel3ListEntry     | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationAdditionalDataIPListEntry               | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| 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.        | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |
| Outbound Events   | This filter identifies events coming from inside the network in your organization targeting the public network.                  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/         |
| ASM Events  | This resource has no description.  | Filter          | ArcSight System/Event Types   |
| Request to Reputation Domains                             | This filter identifies all URL requests to domain names in the reputation domain active list used for real time correlation.     | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/         |

| Resource   | Description  | Type   | URI   |
|--|--|--------|---|
| Dangerous Browsing   | This filter identifies all dangerous browsing activities.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/                       |
| Critical Request Domain Exploit Types  | This filter identifies requested URLs to reputation domain or host name with critical exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/         |
| Dangerous Browsing Request Domain Exploit Types  | This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |
| Critical Target Reputation IP Exploit Types  | This filter identifies critical target reputation IP exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/         |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| 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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |
| Dangerous Outbound Communication   | This filter detects malicious outbound events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/                        |
| Dangerous Browsing Target Reputation IP Exploit Types                                  | This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |

| Resource   | Description  | Type   | URI   |
|--|--|--------|---|
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| Public-Facing Attackers  | This filter identifies all events whose attackers are categorized as public-facing assets.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Interactions with Dangerous Destinations - Rule Firings                                    | This filter identifies all triggered rules that detect interactions with dangerous destinations (non-browsing exploit types).                          | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| Target Host Name Present   | This filter checks if the Target Host Name field is populated.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| ArcSight Internal Events   | This resource has no description.  | Filter | ArcSight System/Event Types   |
| Outbound Communication to Reputation IP Addresses  | This filter identifies all outbound traffic to reputation IP addresses.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Non-ArcSight Internal Events   | This resource has no description.  | Filter | ArcSight System/Event Types   |
| Critical Target Reputation Domain Exploit Types  | This filter identifies critical target reputation domain or host name exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/ |
| 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.      | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| Internal Targets   | This filter identifies events targeting systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |

| Resource  | Description  | Type   | URI   |
|---|--|--------|---|
| Internal Attackers  | This filter identifies events coming from systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/            |
| Dangerous Browsing Activities - Rule Firings                                  | This filter identifies all firings of rules that detect dangerous browsing activities.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| 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.                         | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| 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. | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                     | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| 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.                     | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| 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.   | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| Dangerous Browsing Activities in the Last 24 Hours                            | This query returns all dangerous browsing activities in the last 24 hours.   | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |
| 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.                   | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |



| Resource  | Description  | Type  | URI   |
|---|--|-------|---|
| 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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                                       | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                                     | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                                  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/ |

| Resource   | Description   | Type  | URI   |
|--|---|-------|---|
| 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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/               |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/               |
| 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).  | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/  |

## Event Enrichment with Reputation Data

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-2** Resources that Support the Event Enrichment with Reputation Data Use Case

| Resource                                       | Description  | Type            | URI   |
|--|--|-----------------|---|
| <b>Library Resources</b>                       |  |                 |   |
| Malicious IP Addresses                         | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.                                       | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                 |
| Malicious Domains                              | This active list stores up to 1,500,000 reputation domain names from the RepDV database.                                       | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                 |
| solnGetAttackerReputationDomainLevel2ListEntry | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainLevel4ListEntry   | This variable returns the entry in the reputation domain list corresponding to the target domain level 4.                      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetAttackerReputationHostNameListEntry     | This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel2                  | This variable returns the two rightmost subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerReputationIPListEntry           | This variable returns the attacker address entry in the reputation IP database.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerReputationDomainLevel3ListEntry | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetAttackerDomainLevel3                    | This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.                | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |

| Resource                                       | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetRequestURLDomainLevel4ListEntry         | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.                        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainLevel2ListEntry   | This variable returns the entry in the reputation domain list corresponding to the target domain level 2.                                 | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel1                  | This variable returns the right most subdomain of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLDomainLevel4                  | This variable returns the 4 right most subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetAttackerReputationDomainLevel4ListEntry | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.                               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainLevel3ListEntry   | This variable returns the entry in the reputation domain list corresponding to the target domain level 3.                                 | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainEntry             | This variable returns the entry of a target in the reputation domain list used for real time correlation.                                 | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetRequestURLDomainLevel2ListEntry         | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.                        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetTargetReputationIPListEntry             | This variable returns the target address entry in the reputation IP database.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetLowerTargetHostName                     | This variable returns the target host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |

| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetTargetReputationHostNameListEntry    | This variable returns the entry of a target host name in the reputation domain list used for real time correlation.                                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetDomainLevel3                   | This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetAttackerReputationDomainEntry        | This variable returns the entry of an attacker in the reputation domain list used for real time correlation.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| 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 1.5/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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLDomainLevel3ListEntry      | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.                                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel1ListEntry      | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.                                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomain                     | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |

| Resource                                   | Description   | Type            | URI   |
|--|---|-----------------|---|
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLReputationDomainEntry     | This variable returns the entry of a request URL in the reputation domain list used for real time correlation.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetBaseRequestURLDomainEntry           | This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetDomainLevel2                  | This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.                  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerDomainLevel2                | This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetRequestURLDomainLevel3              | This variable returns the three rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/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 1.5/Event Enrichment with Reputation Data/ |
| solnGetLowerAttackerHostName               | This variable returns the attacker host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetTargetDomainLevel4                  | This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |

| Resource                                | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetAttackerDomainLevel4             | This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                 |
| 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 1.5/                                     |
| 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 1.5/                                     |
| 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 1.5/                                     |
| Events to Malicious Targets             | This filter identifies events whose targets are found in the reputation database.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/Events Enrichment with Reputation Data/ |

## General Scenarios

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-3** Resources that Support the General Scenarios Use Case

| Resource                                 | Description  | Type           | URI  |
|--|--|----------------|--|
| <b>Monitor Resources</b>                 |  |                |  |
| 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 1.5/General Scenarios/ |

| Resource  | Description   | Type         | URI  |
|---|---|--------------|--|
| 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 1.5/General Scenarios/    |
| 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 1.5/General Scenarios/ |
| Communication to Malicious Hosts  | This query viewer displays all outbound malicious communication matches during the last day.                                      | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Communication from Malicious Hosts  | This query viewer displays all inbound malicious communication matches during the last day.                                       | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Events per Scenario   | This query viewer shows the captured events per scenario during the last day.   | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| 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. | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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 1.5/General Scenarios/       |



| Resource  | Description  | Type        | URI   |
|---|--|-------------|---|
| 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 1.5/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 1.5/General Scenarios/      |
| <b>Library Resources</b>                                |  |             |   |
| 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 1.5/General Scenarios/ |
| ArcSight Internal Events                                | This resource has no description.  | Filter      | ArcSight System/Event Types   |
| Dangerous Communication                                 | This filter detects Layer 1 events.  | Filter      | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/      |
| Non-ArcSight Internal Events                            | This resource has no description.  | Filter      | ArcSight System/Event Types   |
| ASM Events  | This resource has no description.  | Filter      | ArcSight System/Event Types   |
| Scenarios Events  | This filter detects Layer 2 events (scenario events); the scenarios found in the Scenarios active list.  | Filter      | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/      |
| Layer 2 Events - Trend Base                             | This query retrieves all of the Layer 2 events during the last day, and is used by a trend.  | Query       | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/      |

| Resource  | Description  | Type  | URI  |
|---|--|-------|--|
| Events per Scenarios During the Last Day -On Trend        | This query retrieves all the scenario events during the last day, grouped by scenario type.                                | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Hourly Count of Outbound Events on the Last Day -On Trend | This query is the base query for Communication to Malicious Hosts during the Last day.                                     | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| 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.                                 | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| 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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Scenario Events During the Last 7 Days-On Trend           | This query retrieves all of the scenario events for the last seven days.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Layer 1 Events - Trend Base                               | This query retrieves all of the layer 1 events during the last hour, and is used by a trend.                               | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| 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.     | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/ |
| Layer 1 Trend   | This trend runs hourly over Layer 1 events (Inbound/Outbound Malicious Communication).                                     | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/  |
| Layer 2 Trend   | This trend runs hourly over Layer 2 events (Scenario events).  | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/  |

## Internal Assets Found in Reputation Data

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-4** Resources that Support the Internal Assets Found in Reputation Data Use Case

| Resource   | Description  | Type         | URI   |
|--|--|--------------|---|
| <b>Monitor Resources</b>                             |  |              |   |
| 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 1.5/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.  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/ |
| All Internal Domains and Hosts Found                 | This query viewer shows all local domain names and hosts appeared in the reputation domain database.   | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/Internal Assets Found in Reputation Data/       |
| <b>Library Resources</b>                             |  |              |   |
| Malicious IP Addresses                               | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.   | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| Internal IP Addresses Found in Reputation Data       | This active list stores all local IP addresses that appear in the reputation IP database.  | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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 hpe.com or hpe.co.uk. | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/  |

| Resource  | Description  | Type        | 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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/Internal Assets Found in Reputation Data/ |
| Malicious Domains   | This active list stores up to 1,500,000 reputation domain names from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/  |
| All Internal Domains Found                                    | This query returns all local domains that appear in the reputation domain database.  | Query       | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/Internal Assets Found in Reputation Data/      |
| All Internal IP Addresses Found                               | This query returns all local IPs that appear in the reputation domain database.  | Query       | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/      |

## Internal Infected Assets

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-5** Resources that Support the Internal Infected Assets Use Case

| Resource  | Description  | Type           | URI   |
|---|--|----------------|---|
| <b>Monitor Resources</b>  |  |                |   |
| 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 1.5/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 1.5/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 1.5/Internal Infected Assets/      |
| Open Case Status Distribution   | This query viewer shows all open cases on internal infected assets, grouped by case status.  | Query Viewer   | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/   |
| Summary of Contacted Malicious Entities                                   | This query viewer shows the summary of malicious hosts contacted by infected internal hosts.   | Query Viewer   | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/   |
| Infected Asset Count per Month  | This query viewer shows the count of internal infected assets per month over the last year.  | Query Viewer   | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Query Viewer   | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/   |

| Resource  | Description  | Type   | URI  |
|---|--|--------|--|
| 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 1.5/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 1.5/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 1.5/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 1.5/Internal Infection Assets/ |
| <b>Library - Correlation Resources</b>                                      |  |        |  |
| 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.   | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/    |
| 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.  | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/    |

| Resource   | Description  | Type        | URI  |
|--|--|-------------|--|
| 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.   | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/            |
| <b>Library Resources</b>   |  |             |  |
| Malicious IP Addresses   | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                              |
| Additional Malicious Domains   | This active list enables user to define reputation domain names.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/ |
| Exceptions - IPs   | This active list enable the user to define entries which will NOT be considered bad.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/ |
| 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 1.5/Internal Infected Assets/     |
| Exceptions - Domains   | This active list enable the user to define entries which will NOT be considered bad.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/     |
| 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.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/     |
| Additional Malicious IP Addresses                                      | This active list enables user to define reputation IP addresses.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/ |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| Malicious Domains  | This active list stores up to 1,500,000 reputation domain names from the RepDV database.                            | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                     |
| Support RepSM Advanced Content                             | This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.   | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                             |
| Protected  | This is a site asset category.  | Asset Category  | /All Asset Categories/Site Asset Categories/Address Spaces  |
| Public-Facing  | This is a solutions asset category.   | Asset Category  | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                                      |
| solnGetTargetReputationDomainLevel4ListEntry               | This variable returns the entry in the reputation domain list corresponding to the target domain level 4.           | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetURLIP   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| 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 1.5/Configuration/                             |
| solnGetRequestURLDomainLevel2                              | This variable returns the two rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGenericHighScoreThreshold                              | This global variable defines the generic threshold for high reputation scores.                                      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |
| solnGetDestinationScore                                    | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetDestinationExceptionHostNameListEntry               | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetDestinationAdditionalDataDomainEntry                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |



| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetDestinationAdditionalDataDomainLevel2ListEntry  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetReputationDomainLevel3ListEntry           | This variable returns the entry in the reputation domain list corresponding to the target domain level 3.           | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainEntry                     | This variable returns the entry of a target in the reputation domain list used for real time correlation.           | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLDomainLevel2ListEntry                 | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationIPListEntry                     | This variable returns the target address entry in the reputation IP database.                                       | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetURLDomain                                       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetLowerTargetHostName                             | This variable returns the target host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainLevel2ListEntry   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetDomainLevel3                              | This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| 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 1.5/Configuration/                             |
| solnGetRequestURLDomain                                | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnCheckDestinationIsInExceptionsDomainList           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetTargetDomainLevel2                            | This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetBaseRequestURLAdditionalDataDomainEntry       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetRequestURLDomainExploitType                   | This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetTargetDomainExploitType                       | This variable returns the exploit type of a target in the reputation domain list used for real time correlation.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetURLScore                                      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetDestinationExceptionDomainLevel3ListEntry     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetDestinationIP                                 | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetURLExploitType                                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetTargetDomainLevel4                            | This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainEntry           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLAdditionalDataDomainLevel4ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |

| Resource  | Description   | Type            | URI   |
|---|---|-----------------|---|
| solnGetDestinationAdditionalDataDomainLevel4ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationExceptionDomainLevel4ListEntry      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetLowerDestinationHostName                       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainLevel4ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainLevel2ListEntry          | This variable returns the entry in the reputation domain list corresponding to the target domain level 2.           | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetDestinationAdditionalDataHostNameListEntry     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetRequestURLDomainLevel1                         | This variable returns the right most subdomain of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainLevel4                         | This variable returns the 4 right most subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationDomain                              | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetTargetReputationHostNameListEntry              | This variable returns the entry of a target host name in the reputation domain list used for real time correlation. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetDestinationExploitType                         | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |

| Resource  | Description   | Type            | URI  |
|---|---|-----------------|--|
| solnGetDestinationExceptionDomainLevel2ListEntry      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/           |
| solnNullAddresses                                     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                            |
| solnGetDestinationExceptionIPListEntry                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/               |
| solnGetRequestURLDomainLevel3ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                    |
| solnGetRequestURLDomainLevel1ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                    |
| solnGetRequestURLReputationDomainEntry                | This variable returns the entry of a request URL in the reputation domain list used for real time correlation.      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/               |
| solnGetRequestURLAdditionalDataDomainLevel3ListEntry  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                    |
| solnGetRequestURLDomainLevel3                         | This variable returns the three rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                            |
| solnGetDestinationAdditionalDataDomainLevel3ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/ |
| solnGetDestinationAdditionalDataIPListEntry           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/               |
| Standard  | This resource has no description.   | Field Set       | ArcSight System/Event Field Sets/Active Channels   |

| Resource   | Description  | Type      | URI   |
|--|--|-----------|---|
| Internal Infections  | This field set provides the fields relevant to the correlation events generated by the detection rules in this use case.   | Field Set | /All Field Sets/ArcSight Solutions/Reputation Security Monitor 1.5/                               |
| Public-Facing Attackers                                      | This filter identifies all events whose attackers are categorized as public-facing assets.   | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Outbound Events  | This filter identifies events coming from inside the network in your organization targeting the public network.  | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| 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.   | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Target Host Name Present                                     | This filter checks if the Target Host Name field is populated.   | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Request to Reputation Domains                                | This filter identifies all URL requests to domain names in the reputation domain active list used for real time correlation.   | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| 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.     | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| Critical Request Domain Exploit Types                        | This filter identifies requested URLs to reputation domain or host name with critical exploit types.   | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/ |
| Critical Target Reputation IP Exploit Types                  | This filter identifies critical target reputation IP exploit types.  | Filter    | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/ |

| Resource   | Description  | Type   | URI   |
|--|--|--------|---|
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| 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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| Outbound Communication to Reputation IP Addresses                          | This filter identifies all outbound traffic to reputation IP addresses.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Critical Target Reputation Domain Exploit Types                            | This filter identifies critical target reputation domain or host name exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/ |
| Internal Attackers   | This filter identifies events coming from systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Internal Targets   | This filter identifies events targeting systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Summary of Currently Infected Assets                                       | This query returns the summary of internal infected machines detected through communications with reputation IP addresses or domains.  | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| 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.  | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |

| Resource  | Description  | Type  | URI   |
|---|--|-------|---|
| Currently Infected Assets and Recorded Interactions with Malicious Entities | This query returns all internal infected assets detected through communications with reputation IPs or domains.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| 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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| Infection Types over Last Month   | This query returns the weekly count of internal infected assets over the last month.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| Internal Infected Asset Count per Month                                     | This query returns the count of internal infected assets detected per month over the last year.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| Summary of Contacted Malicious Hosts  | This query returns the summary of malicious hosts contacted by infected internal hosts.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| Internal Infected Asset Count per Week                                      | This query returns the weekly count of internal infected assets detected during the last month.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/ |
| Daily Internal Infected Asset Snapshots                                     | This trend stores snapshots of the internal infected asset list on a daily basis.  | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/  |

## RepSM Overview

The following table lists resources explicitly assigned to this use case and any dependant resources.

**Table D-6** Resources that Support the RepSM Overview Use Case

| Resource   | Description   | Type         | URI  |
|--|---|--------------|--|
| <b>Monitor Resources</b>   |   |              |  |
| RepSM Overview   | This dashboard provides an overview of traffic from reputation hosts in the last 24 hours (not real time).  | Dashboard    | /All Dashboards/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                                   |
| Geographical View of Malicious Communications  | This dashboard provides an overview of traffic to reputation hosts.   | Dashboard    | /All Dashboards/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                                   |
| 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.   | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                                |
| 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.   | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/           |
| <b>Library - Correlation Resources</b>   |   |              |  |
| Access from Dangerous Sources: Inbound Communications from Malicious IPs                     | This rule captures the inbound communication to internal assets, from reputation IP addresses. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious IP.        | Rule         | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/Access from Dangerous Sources/ |
| 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. | Rule         | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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.                 | Rule         | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                                |



| Resource  | Description  | Type        | URI  |
|---|--|-------------|--|
| 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.                  | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                                |
| Access from Dangerous Sources: Inbound Communications from Malicious Domains                  | This rule captures inbound communications to internal assets, from reputation domain names. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious Domain.        | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/Access from Dangerous Sources/ |
| <b>Library Resources</b>  |  |             |  |
| Malicious IP Addresses  | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/  |
| Additional Malicious Domains  | This active list enables user to define reputation domain names.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/             |
| 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 1.5/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.                                | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/            |

| Resource  | Description   | Type           | URI  |
|---|---|----------------|--|
| 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. | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/    |
| Exceptions - IPs  | This active list enable the user to define entries which will NOT be considered bad.  | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| 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 1.5/Access to Dangerous Destinations/ |
| Exceptions - Domains  | This active list enable the user to define entries which will NOT be considered bad.  | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| Additional Malicious IP Addresses                                     | This active list enables user to define reputation IP addresses.  | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| Malicious Domains   | This active list stores up to 1,500,000 reputation domain names from the RepDV database.  | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                  |
| Support RepSM Advanced Content  | This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.   | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                          |
| Protected   | This is a site asset category.  | Asset Category | /All Asset Categories/Site Asset Categories/Address Spaces   |
| Public-Facing   | This is a solutions asset category.   | Asset Category | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                                   |
| Internal Non Public-Facing  | This is a solutions asset category.   | Asset Category | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                                   |
| 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.   | Data Monitor   | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                        |
| Access to Malicious Entities  | This data monitor shows a geographical view of all (successful or failed) access to malicious hosts or IP addresses.  | Data Monitor   | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                        |

| Resource                                       | Description  | Type            | URI   |
|--|--|-----------------|---|
| Attacks from Malicious Entities                | This data monitor shows a geographical view of all successful and failed inbound communications from malicious hosts or IP addresses.                          | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                       |
| 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. | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                       |
| Recent Dangerous Browsing Destinations         | This data monitor shows the last 20 dangerous browsing destinations from non public-facing internal assets.  | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                       |
| solnGetAttackerReputationDomainLevel2ListEntry | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainLevel4ListEntry   | This variable returns the entry in the reputation domain list corresponding to the target domain level 4.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetAttackerReputationHostNameListEntry     | This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel2                  | This variable returns the two rightmost subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGenericHighScoreThreshold                  | This global variable defines the generic threshold for high reputation scores.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                         |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerReputationIPListEntry           | This variable returns the attacker address entry in the reputation IP database.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceDomain                            | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/  |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| 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 1.5/Configuration/                         |
| solnGetDestinationExceptionHostNameListEntry          | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/              |
| solnGetDestinationAdditionalDataDomainEntry           | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetDestinationAdditionalDataDomainLevel2ListEntry | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/    |
| solnGetLowerSourceHostName                            | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerReputationDomainLevel4ListEntry        | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.                      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainLevel3ListEntry          | This variable returns the entry in the reputation domain list corresponding to the target domain level 3.                        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationDomainEntry                    | This variable returns the entry of a target in the reputation domain list used for real time correlation.                        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetRequestURLDomainLevel2ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetTargetReputationIPListEntry                    | This variable returns the target address entry in the reputation IP database.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetLowerTargetHostName                            | This variable returns the target host name in lower case.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |

| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetSource Score                                 | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/  |
| solnGetTarget DomainLevel3                          | This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetSource AddirionalData IPListEntry            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetAttackerReputationDomainEntry                | This variable returns the entry of an attacker in the reputation domain list used for real time correlation.                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSource AdditionalData DomainEntry            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| 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 1.5/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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLDomain                             | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetSource AdditionalData DomainLevel3 ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/    |

| Resource  | Description   | Type            | URI   |
|---|---|-----------------|---|
| solnCheckDestinationIsInExceptionsDomainList                    | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetTargetDomainLevel2                                       | This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| 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 1.5/Event Enrichment with Reputation Data/     |
| solnGetSourceExploitType  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/      |
| solnGetDestinationIP  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetDestinationExceptionDomainLevel3ListEntry                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| 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 1.5/Event Enrichment with Reputation Data/     |
| solnGetAttackerDomainLevel4                                     | This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.            | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetTargetDomainLevel4                                       | This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainLevel4ListEntry            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |

| Resource  | Description   | Type            | URI   |
|---|---|-----------------|---|
| solnGetDestinationAdditionalDataDomainLevel4ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/    |
| solnGetDestinationExceptionDomainLevel4ListEntry      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/              |
| solnGetLowerDestinationHostName                       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetAttackerReputationDomainLevel3ListEntry        | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.                 | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel4ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetAttackerDomainLevel3                           | This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.             | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Configuration/                         |
| solnGetDestinationAdditionalDataHostNameListEntry     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/    |
| solnGetTargetReputationDomainLevel2ListEntry          | This variable returns the entry in the reputation domain list corresponding to the target domain level 2.                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetRequestURLDomainLevel1                         | This variable returns the right most subdomain of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetRequestURLDomainLevel4                         | This variable returns the 4 right most subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |

| Resource  | Description   | Type            | URI   |
|---|---|-----------------|---|
| solnGetSourceAdditionalDataHostNameListEntry                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationDomain                                    | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| 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.                              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |
| solnGetTargetReputationHostNameListEntry                    | This variable returns the entry of a target host name in the reputation domain list used for real time correlation.                                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnNullAddresses   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationExceptionDomainLevel2ListEntry            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetAttackerDomainExploitType                            | This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.                                   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetDestinationExceptionIPLISTEntry                      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetSourceIP   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/      |
| 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 1.5/Event Enrichment with Reputation Data/     |
| solnGetRequestURLDomainLevel3ListEntry                      | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.                                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |



| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetRequestURLDomainLevel1ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.       | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLReputationDomainEntry                | This variable returns the entry of a request URL in the reputation domain list used for real time correlation.           | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceAdditionalDataDomainLevel2ListEntry      | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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.      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGetAttackerDomainLevel2                           | This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.            | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetRequestURLDomainLevel3                         | This variable returns the three rightmost subdomains of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetLowerAttackerHostName                          | This variable returns the attacker host name in lower case.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetDestinationAdditionalDataDomainLevel3ListEntry | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/    |
| solnGetDestinationAdditionalDataIPListEntry           | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| Events with Target Reputation Information             | This field set contains fields with target reputation domain or IP address information.                                  | Field Set       | /All Field Sets/ArcSight Solutions/Reputation Security Monitor 1.5/                                   |
| Events with Source Reputation Information             | This field set contains fields with source reputation domain or IP address information.                                  | Field Set       | /All Field Sets/ArcSight Solutions/Reputation Security Monitor 1.5/                                   |

| Resource  | Description  | Type   | URI   |
|---|--|--------|---|
| Inbound Events                                    | This filter identifies events coming from outside your network, targeting your organization.                                     | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Non Public-Facing Internal Targets                | This filter identifies all events for which the targets are categorized as non public-facing internal.                           | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Inbound Communication from Malicious Domains      | This filter identifies all inbound traffic from domain names in the reputation domain active list.                               | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Outbound Events                                   | This filter identifies events coming from inside the network in your organization targeting the public network.                  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Reputation Outbound Communication                 | This filter identifies all communication to a malicious host or IP address.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                         |
| Reputation Inbound Communication                  | This filter identifies all events from a malicious host or IP address.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                         |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| ASM Events  | This resource has no description.  | Filter | ArcSight System/Event Types   |
| Target Host Name Present                          | This filter checks if the Target Host Name field is populated.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Dangerous Browsing                                | This filter identifies all dangerous browsing activities.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/               |
| 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.         | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Internal Infected Asset Case Creation or Removal  | This filter identifies events generated when the active list storing internal infection records is modified.                     | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                         |

| Resource  | Description  | Type   | URI   |
|---|--|--------|---|
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| ArcSight Internal Events                          | This resource has no description.  | Filter | ArcSight System/Event Types   |
| Outbound Communication to Reputation IP Addresses | This filter identifies all outbound traffic to reputation IP addresses.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| Non-ArcSight Internal Events                      | This resource has no description.  | Filter | ArcSight System/Event Types   |
| Zero Day Attack List Manipulation                 | This filter identifies events generated when the active list storing zero day attack records is modified.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                         |
| Zero Day Attack Reputation Domain Exploit Types   | This filter identifies events from malicious domain names or host names with zero-day attack exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| Zero Day Attack Reputation IP Exploit Types       | This filter identifies events from malicious IP addresses with zero day attack exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| Internal Attackers                                | This filter identifies events coming from systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Internal Targets                                  | This filter identifies events targeting systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Dangerous Outbound Communication                  | This filter detects malicious outbound events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/                |
| Dangerous Browsing Activities - Rule Firings      | This filter identifies all firings of rules that detect dangerous browsing activities.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/               |

| Resource   | Description   | Type  | URI   |
|--|---|-------|---|
| 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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                 |
| 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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Overview/                         |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                                       | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/    |
| 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.   | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/     |
| 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).  | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/  |

## RepSM Package Health Status

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-7** Resources that Support the RepSM Package Health Status Use Case

| Resource                           | Description   | Type      | URI   |
|------------------------------------|---|-----------|---|
| <b>Monitor Resources</b>           |   |           |   |
| 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 1.5/RepSM Package Health Status/ |

| Resource  | Description  | Type      | URI   |
|---|--|-----------|---|
| 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 1.5/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 1.5/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 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 1.5/RepSM Package Health Status/ |
| <b>Library - Correlation Resources</b>  |  |           |   |
| 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.  | Rule      | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| 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.  | Rule      | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/    |
| 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.  | Rule      | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Rule      | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                 |

| Resource  | Description  | Type | URI   |
|---|--|------|---|
| Internal Domain Found in Reputation Data  | This rule detects when an internal domain appears in the reputation domain database.   | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/ |
| 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.  | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |
| 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. | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                         |
| 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.   | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/            |
| Internal IP Address Found in Reputation Data  | This rule detects when an internal address appears in the reputation IP database.  | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Assets Found in Reputation Data/ |
| 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.  | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |
| 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.  | Rule | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                         |

| Resource   | Description   | Type        | URI   |
|--|---|-------------|---|
| 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.                    | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/             |
| 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.     | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/             |
| 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.          | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/             |
| <b>Library Resources</b>   |   |             |   |
| 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 1.5/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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/ |
| 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.       | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/ |
| 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 1.5/Internal Infected Assets/      |

| Resource  | Description  | Type        | URI  |
|---|--|-------------|--|
| 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. | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| Exceptions - Domains  | This active list enable the user to define entries which will NOT be considered bad.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| 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 1.5/Access to Dangerous Destinations/ |
| Malicious Domains   | This active list stores up to 1,500,000 reputation domain names from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                  |
| Malicious IP Addresses  | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                  |
| Additional Malicious Domains  | This active list enables user to define reputation domain names.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| Exceptions - IPs  | This active list enable the user to define entries which will NOT be considered bad.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |
| 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.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| Additional Malicious IP Addresses   | This active list enables user to define reputation IP addresses.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/     |



| Resource   | Description   | Type           | 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. | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/          |
| Support RepSM Advanced Content                               | This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.   | Active List    | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| Protected  | This is a site asset category.  | Asset Category | /All Asset Categories/Site Asset Categories/Address Spaces  |
| Public-Facing  | This is a solutions asset category.   | Asset Category | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor  |
| Internal Non Public-Facing                                   | This is a solutions asset category.   | Asset Category | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor  |
| Last 10 RepSM Trend Query Failures                           | This data monitor shows the last 10 trend query failures.   | Data Monitor   | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Trend 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.   | Data Monitor   | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Data Monitor   | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Trend Health/ |

| Resource   | Description   | Type         | URI   |
|--|---|--------------|---|
| Last 10 RepSM Trend Queries Returning No Results                           | This data monitor shows the last 10 trend queries that returned no results.   | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Trend Health/     |
| RepSM Rule States  | This data monitor shows the last state of the RepSM rules as either enabled, disabled or deleted.   | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Rule Health/      |
| 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.                                 | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Event Statistics/ |
| Top Firing Rules   | This data monitor shows the reputation traffic monitoring rule with most triggerings.   | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Rule Health/      |
| 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. | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Event Statistics/ |
| 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.  | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Rule Health/      |
| 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.  | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Event Statistics/ |
| Recently Triggered Rules   | This data monitor shows the 10 recent RepSM rule triggerings.   | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Rule Health/      |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| 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.                                       | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Event Statistics/ |
| 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. | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/Event Statistics/ |
| solnGetAttackerReputationDomainLevel2ListEntry                 | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainLevel4ListEntry                   | This variable returns the entry in the reputation domain list corresponding to the target domain level 4.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetAttackerReputationHostNameListEntry                     | This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetURLIP   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/           |
| 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 1.5/Configuration/                                       |
| solnGetRequestURLDomainLevel2                                  | This variable returns the two rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/   |
| solnGenericHighScoreThreshold                                  | This global variable defines the generic threshold for high reputation scores.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                                       |
| solnGetAttackerReputationIPListEntry                           | This variable returns the attacker address entry in the reputation IP database.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                                |
| 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.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                                       |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetSourceDomain                                   | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/      |
| 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 1.5/Configuration/                             |
| solnGetDestinationScore                               | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetDestinationExceptionHostNameListEntry          | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetDestinationAdditionalDataDomainEntry           | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetDestinationAdditionalDataDomainLevel2ListEntry | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetLowerSourceHostName                            | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetAttackerReputationDomainLevel4ListEntry        | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainLevel3ListEntry          | This variable returns the entry in the reputation domain list corresponding to the target domain level 3.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationDomainEntry                    | This variable returns the entry of a target in the reputation domain list used for real time correlation.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetRequestURLDomainLevel2ListEntry                | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetTargetReputationIPListEntry                    | This variable returns the target address entry in the reputation IP database.                                      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnGetURLDomain                                       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetLowerTargetHostName                             | This variable returns the target host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLAdditionalDataDomainLevel2ListEntry   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetSourceScore                                     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/      |
| solnGetTargetDomainLevel3                              | This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetSourceAdditionalDataIPLISTEntry                 | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetAttackerReputationDomainEntry                   | This variable returns the entry of an attacker in the reputation domain list used for real time correlation.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetSourceAdditionalDataDomainEntry                 | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| 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 1.5/Configuration/                             |
| solnGetRequestURLDomain                                | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetSourceAdditionalDataDomainLevel3ListEntry       | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |

| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnCheckDestinationIsInExceptionsDomainList     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetBaseRequestURLAdditionalDataDomainEntry   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetDomainLevel2                        | This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainExploitType               | This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetTargetDomainExploitType                   | This variable returns the exploit type of a target in the reputation domain list used for real time correlation.        | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| solnGetURLScore                                  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetDestinationIP                             | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnGetSourceExploitType                         | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/      |
| solnGetDestinationExceptionDomainLevel3ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |
| solnGetURLExploitType                            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By URL Request/ |
| solnGetAttackerDomainLevel4                      | This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.            | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |

| Resource  | Description   | Type            | URI  |
|---|---|-----------------|--|
| solnGetTargetDomainLevel4                                       | This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                            |
| solnGetRequestURLAdditionalDataDomainEntry                      | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/               |
| solnGetRequestURLAdditionalDataDomainLevel4ListEntry            | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/ |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                      |
| solnGetDestinationAdditionalDataDomainLevel4ListEntry           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/ |
| solnGetDestinationExceptionDomainLevel4ListEntry                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/           |
| solnGetLowerDestinationHostName                                 | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                            |
| solnGetAttackerReputationDomainLevel3ListEntry                  | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.             | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                    |
| solnGetRequestURLDomainLevel4ListEntry                          | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                    |
| solnGetAttackerDomainLevel3                                     | This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                            |
| 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 1.5/Configuration/                      |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetDestinationAdditionalDataHostNameListEntry           | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetTargetReputationDomainLevel2ListEntry                | This variable returns the entry in the reputation domain list corresponding to the target domain level 2.                | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetRequestURLDomainLevel1                               | This variable returns the right most subdomain of the requested URL.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetRequestURLDomainLevel4                               | This variable returns the 4 right most subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetSourceAdditionalDataHostNameListEntry                | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationDomain                                    | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                             |
| solnGetTargetReputationHostNameListEntry                    | This variable returns the entry of a target host name in the reputation domain list used for real time correlation.      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/   |
| solnGetDestinationExploitType                               | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Destination/ |
| solnNullAddresses   | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationExceptionDomainLevel2ListEntry            | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Exceptions/                  |



| Resource   | Description   | Type            | URI  |
|--|---|-----------------|--|
| solnGetAttackerDomainExploitType                                   | This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                 |
| solnGetDestinationExceptionIPListEntry                             | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                 |
| solnGetSourceIP  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/ |
| solnGetRequestURLDomainLevel3ListEntry                             | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                        |
| solnGetRequestURLDomainLevel1ListEntry                             | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| solnGetRequestURLReputationDomainEntry                             | This variable returns the entry of a request URL in the reputation domain list used for real time correlation.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                 |
| solnGetSourceAdditionalDataDomainLevel2ListEntry                   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/   |
| solnGetRequestURLAdditionalDataDomainLevel3ListEntry               | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/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.         | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| solnGetAttackerDomainLevel2  | This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.               | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetRequestURLDomainLevel3                                      | This variable returns the three rightmost subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |

| Resource  | Description  | Type            | URI   |
|---|--|-----------------|---|
| solnGetLowerAttackerHostName                              | This variable returns the attacker host name in lower case.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                                   |
| solnGetDestinationAdditionalDataDomainLevel3ListEntry     | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/        |
| solnGetDestinationAdditionalDataIPListEntry               | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                      |
| Inbound Events  | This filter identifies events coming from outside your network, targeting your organization.   | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| 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.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |
| Non Public-Facing Internal Targets                        | This filter identifies all events for which the targets are categorized as non public-facing internal.   | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| Outbound Events   | This filter identifies events coming from inside the network in your organization targeting the public network.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| Events from Model Import Connector for RepSM              | This filter identifies important events generated by the RepSM Model Import Connector.   | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/              |
| 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.   | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/         |
| RepSM Trend Runs Status                                   | This filter identifies trend query run events.   | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/              |
| ASM Events  | This resource has no description.  | Filter          | ArcSight System/Event Types   |
| 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. | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/                 |

| Resource   | Description  | Type   | URI   |
|--|--|--------|---|
| Request to Reputation Domains  | This filter identifies all URL requests to domain names in the reputation domain active list used for real time correlation.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/         |
| Dangerous Browsing Request Domain Exploit Types  | This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |
| Critical Request Domain Exploit Types  | This filter identifies requested URLs to reputation domain or host name with critical exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/         |
| Critical Target Reputation IP Exploit Types  | This filter identifies critical target reputation IP exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/         |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| 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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |
| 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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/              |
| Dangerous Outbound Communication   | This filter detects malicious outbound events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/                        |

| Resource  | Description  | Type   | URI   |
|---|--|--------|---|
| Dangerous Browsing Target Reputation IP Exploit Types                                     | This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/Support/ |
| 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.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/              |
| Public-Facing Attackers   | This filter identifies all events whose attackers are categorized as public-facing assets.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                                  |
| Inbound Communication from Malicious Domains  | This filter identifies all inbound traffic from domain names in the reputation domain active list.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/         |
| Zero Day Attacks - Rule Firings   | This filter identifies all correlation events generated by rules that detect zero day attacks.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                         |
| 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.                               | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/                 |
| RepSM Rule Firing Events  | This filter identifies all triggerings of RepSM rules.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/              |
| Interactions with Dangerous Destinations - Rule Firings                                   | This filter identifies all triggered rules that detect interactions with dangerous destinations (non-browsing exploit types).  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/         |

| Resource  | Description   | Type   | URI   |
|---|---|--------|---|
| RepSM Trend Query Duration                                  | This filter identifies successful RepSM trend query run events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/      |
| RepSM Trend Query Failure                                   | This filter identifies failed RepSM trend query run events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/      |
| Dangerous Inbound Communication                             | This filter detects malicious inbound events.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/                |
| Target Host Name Present                                    | This filter checks if the Target Host Name field is populated.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| 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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| 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.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/      |
| Access from Dangerous Sources - Rule Firings                | This filter identifies all correlation events generated by rules that detect access from dangerous sources.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/    |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/         |
| Outbound Communication to Reputation IP Addresses           | This filter identifies all outbound traffic to reputation IP addresses.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| ArcSight Internal Events                                    | This resource has no description.   | Filter | ArcSight System/Event Types   |

| Resource   | Description   | Type   | URI   |
|--|---|--------|---|
| Non-ArcSight Internal Events   | This resource has no description.   | Filter | ArcSight System/Event Types   |
| Critical Target Reputation Domain Exploit Types  | This filter identifies critical target reputation domain or host name exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Internal Infected Assets/Support/ |
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/      |
| RepSM Rules Engine Events  | This filter identifies all internal audit events related to RepSM rules.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/RepSM Package Health Status/      |
| Zero Day Attack Reputation Domain Exploit Types  | This filter identifies events from malicious domain names or host names with zero-day attack exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| 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.                               | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Access to Dangerous Destinations/ |
| Zero Day Attack Reputation IP Exploit Types  | This filter identifies events from malicious IP addresses with zero day attack exploit types.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| Internal Targets   | This filter identifies events targeting systems inside the network in your organization.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Internal Attackers   | This filter identifies events coming from systems inside the network in your organization.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Dangerous Browsing Activities - Rule Firings   | This filter identifies all firings of rules that detect dangerous browsing activities.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Dangerous Browsing/               |

# Reputation Data Analysis

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-8** Resources that Support the Reputation Data Analysis Use Case

| Resource                            | Description  | Type         | URI   |
|-------------------------------------|--|--------------|---|
| <b>Monitor Resources</b>            |  |              |   |
| 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 1.5/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 1.5/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 1.5/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 1.5/Reputation Data Analysis/ |
| Reputation IP Entry Count           | This query viewer shows the current number of reputation addresses.  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| Reputation Domain Score Histogram   | This query viewer shows the histogram of the reputation domain score.  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| Reputation IP Score Histogram       | This query viewer shows the histogram of the reputation IP score.  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |

| Resource   | Description   | Type         | URI   |
|--|---|--------------|---|
| Reputation IP Exploit Type Distribution                                    | This query viewer shows the reputation address count per exploit type.                    | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| Reputation Domain Exploit Type Distribution                                | This query viewer shows the reputation domain count per exploit type.                     | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| Reputation Domain Type Distribution  | This query viewer shows the distribution of entries in the reputation domain database.    | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/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. | Report       | /All Reports/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/Reputation Data Analysis/       |
| <b>Library Resources</b>   |   |              |   |
| Malicious IP Addresses   | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.  | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                           |



| Resource   | Description   | Type         | URI   |
|--|---|--------------|---|
| Malicious Domains                                | This active list stores up to 1,500,000 reputation domain names from the RepDV database.  | Active List  | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                           |
| 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.  | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| 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.   | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| 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. | Data Monitor | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/ |
| Reputation Domain Changes                        | This filter identifies events that indicate a change was made to the reputation domain active list.   | Filter       | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/   |
| Reputation IP Changes                            | This filter identifies events that indicate a change was made to the reputation IP address active list.   | Filter       | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/   |
| Reputation IP Entry Count                        | This query returns the current number of reputation addresses.  | Query        | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Query        | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/   |

| Resource   | Description  | Type  | URI   |
|--|--|-------|---|
| Reputation Domain Changes by Type During the Last 1 Week           | This query returns the count of reputation domain exploit types during the last week.            | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Entry Count by Type                              | This query returns the current count of reputation domains and host names.                       | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation IP Entries  | This query returns the top 1,500,000 IP entries in the reputation IP active list.                | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Count - Trend Base                               | This query returns the count of reputation domains, grouped by the exploit type and domain type. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Entries  | This query returns the top 1,500,000 domain entries in the reputation domain active list.        | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Score Histogram                                  | This query builds the histogram of the reputation domain score.                                  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Changes During the Last 1 Week                   | This query returns the count of reputation domain entries during the last week.                  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |

| Resource   | Description   | Type  | URI   |
|--|---|-------|---|
| 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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation IP Score Histogram  | This query builds the histogram of the reputation IP score.                                     | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.               | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation IP by Exploit Type  | This query returns the count of reputation addresses per exploit type.                          | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation IP Changes - Trend Base                                       | This query returns the count of reputation addresses, grouped by the exploit type.              | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain by Exploit Type  | This query returns the reputation domain count per exploit type.                                | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation IP Changes During the Last 1 Week                             | This query returns the count of reputation addresses during the last week.                      | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Database Analysis/ |
| Reputation Domain Changes  | This trend stores the daily count of reputation domain names, grouped by the exploit type.      | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/      |
| Reputation IP changes  | This trend stores the daily count of reputation IP entries, grouped by the exploit type.        | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Reputation Data Analysis/      |

## Zero Day Attacks

The following table lists all the resources explicitly assigned to this use case and any dependant resources.

**Table D-9** Resources that Support the Zero Day Attacks Use Case

| Resource                                     | Description  | Type         | URI   |
|--|--|--------------|---|
| <b>Monitor Resources</b>                     |  |              |   |
| 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 1.5/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  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| Zero Day Attack Cases                        | This query viewer shows all open cases for zero day attacks, grouped by case status.   | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.  | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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. | Query Viewer | /All Query Viewers/ArcSight Solutions/Reputation Security Monitor 1.5/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 1.5/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 1.5/Zero Day Attacks/       |

| Resource   | Description   | Type   | URI  |
|--|---|--------|--|
| 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 1.5/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 1.5/Zero Day Attacks/                              |
| <b>Library - Correlation Resources</b>   |   |        |  |
| Access from Dangerous Sources: Inbound Communications from Malicious IPs                     | This rule captures the inbound communication to internal assets, from reputation IP addresses. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious IP.        | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/Access from Dangerous Sources/ |
| 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. | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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.                 | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/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.                 | Rule   | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                                |

| Resource  | Description  | Type        | URI  |
|---|--|-------------|--|
| 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. | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                                |
| Access from Dangerous Sources: Inbound Communications from Malicious Domains                  | This rule captures inbound communications to internal assets, from reputation domain names. The rule generates correlation events per malicious inbound communication with the scenario type Inbound Communication from Malicious Domain.        | Rule        | /All Rules/ArcSight Solutions/Reputation Security Monitor 1.5/General Scenarios/Access from Dangerous Sources/ |
| <b>Library Resources</b>  |  |             |  |
| Malicious IP Addresses  | This active list stores up to 1,500,000 reputation IP addresses from the RepDV database.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/  |
| Additional Malicious Domains  | This active list enables user to define reputation domain names.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/             |
| 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 1.5/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.                                | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/            |
| 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.                                      | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/            |
| Additional Malicious IP Addresses   | This active list enables user to define reputation IP addresses.   | Active List | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/User Defined Reputation Data/             |

| Resource  | Description   | Type            | URI   |
|---|---|-----------------|---|
| Malicious Domains   | This active list stores up to 1,500,000 reputation domain names from the RepDV database.                                    | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/                                 |
| Support RepSM Advanced Content                                  | This list is support the content logic - DO NOT MODIFY OR CHANGE THIS LIST.   | Active List     | /All Active Lists/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                         |
| Protected   | This is a site asset category.  | Asset Category  | /All Asset Categories/Site Asset Categories/Address Spaces  |
| Internal Non Public-Facing                                      | This is a solutions asset category.   | Asset Category  | /All Asset Categories/ArcSight Solutions/Reputation Security Monitor                                  |
| Most Recent Zero Day Attacks                                    | This data monitor shows the last 20 zero day attacks to non public-facing internal assets.                                  | Data Monitor    | /All Data Monitors/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/               |
| solnGetAttackerReputationDomainLevel2ListEntry                  | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.                 | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| 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.     | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                         |
| solnGetAttackerReputationHostNameListEntry                      | This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.      | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                       |
| solnGenericHighScoreThreshold                                   | This global variable defines the generic threshold for high reputation scores.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                         |
| solnGetAttackerReputationIPListEntry                            | This variable returns the attacker address entry in the reputation IP database.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceDomain   | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/  |
| 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 1.5/Event Enrichment with Reputation Data/ |

| Resource  | Description  | Type            | URI  |
|---|--|-----------------|--|
| 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 1.5/Configuration/                        |
| solnGetAttackerReputationDomainLevel3ListEntry              | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| solnGetAttackerDomainLevel3                                 | This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.          | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetRequestURLDomainLevel4ListEntry                      | This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.       | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| 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 1.5/Configuration/                        |
| solnGetLowerSourceHostName                                  | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetRequestURLDomainLevel4                               | This variable returns the 4 right most subdomains of the requested URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetAttackerReputationDomainLevel4ListEntry              | This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.              | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/                                      |
| solnGetSourceAdditionalDataHostNameListEntry                | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/   |
| 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. | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Configuration/                        |
| solnGetSourceScore  | This resource has no description.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/ |



| Resource   | Description   | Type            | URI   |
|--|---|-----------------|---|
| solnNullAddresses                                | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| solnGetAttackerDomainExploitType                 | This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.             | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetAttackerReputationDomainEntry             | This variable returns the entry of an attacker in the reputation domain list used for real time correlation.                    | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceAdditionalDataIPLISTEntry           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceAdditionalDataDomainEntry           | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/                  |
| solnGetSourceIP                                  | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/  |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetRequestURLDomain                          | This variable returns the domain substring of a request URL.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                               |
| 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 1.5/Event Enrichment with Reputation Data/ |
| solnGetSourceAdditionalDataDomainLevel2ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User 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 1.5/Event Enrichment with Reputation Data/ |

| Resource   | Description   | Type            | URI  |
|--|---|-----------------|--|
| solnGetSourceAdditionalDataDomainLevel3ListEntry     | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/   |
| solnGetAttackerDomainLevel2                          | This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetSourceExploitType                             | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Main Final Variables/Entry By Source/ |
| solnGetLowerAttackerHostName                         | This variable returns the attacker host name in lower case.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetAttackerDomainLevel4                          | This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.  | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/                              |
| solnGetRequestURLAdditionalDataDomainLevel4ListEntry | This resource has no description.   | Global Variable | /All Fields/ArcSight Solutions/Reputation Security Monitor 1.5/Support/Check Additional User Data/   |
| Inbound Events                                       | This filter identifies events coming from outside your network, targeting your organization.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                             |
| 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. | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                    |
| Non Public-Facing Internal Targets                   | This filter identifies all events for which the targets are categorized as non public-facing internal.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                             |
| Inbound Communication from Malicious Domains         | This filter identifies all inbound traffic from domain names in the reputation domain active list.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/    |
| Zero Day Attacks - Rule Firings                      | This filter identifies all correlation events generated by rules that detect zero day attacks.  | Filter          | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                    |

| Resource   | Description  | Type   | URI   |
|--|--|--------|---|
| 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. | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Zero Day Attack Reputation Domain Exploit Types                            | This filter identifies events from malicious domain names or host names with zero-day attack exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| Zero Day Attack Reputation IP Exploit Types                                | This filter identifies events from malicious IP addresses with zero day attack exploit types.  | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/Support/         |
| Internal Targets   | This filter identifies events targeting systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| Internal Attackers   | This filter identifies events coming from systems inside the network in your organization.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/                          |
| 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.   | Filter | /All Filters/ArcSight Solutions/Reputation Security Monitor 1.5/General/Malicious Communications/ |
| 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.  | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                 |
| 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.   | Query  | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/                 |

| Resource  | Description  | Type  | URI   |
|---|--|-------|---|
| Status Distribution of Open Case on Zero Day Attacks                          | This query returns all open cases on zero day attacks, grouped by case status.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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. | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| Zero Day Attacks in the Last 24 Hours   | This query returns all zero day attacks in the last 24 hours.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |

| Resource  | Description  | Type  | URI   |
|---|--|-------|---|
| 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.          | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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 | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.                               | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.                          | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.  | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/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.             | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| Top Attacked Assets During the Last 24 Hours                    | This query returns the internal assets attacked most during the last 24 hours.   | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |
| 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.       | Query | /All Queries/ArcSight Solutions/Reputation Security Monitor 1.5/Zero Day Attacks/ |

| Resource   | Description   | Type  | URI   |
|--|---|-------|---|
| 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. | Trend | /All Trends/ArcSight Solutions/Reputation Security Monitor 1.5/Access from Dangerous Sources/ |