Solution Guide

HP Reputation Security Monitor 1.01

ArcSight ESM and ArcSight Express

March 6, 2013

ArcSight
An HP Company

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI.
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
3/6/2013	Reputation Security Monitor Solution 1.01	Final revision for release.

Contents

Chapter 1

Overview and Architecture

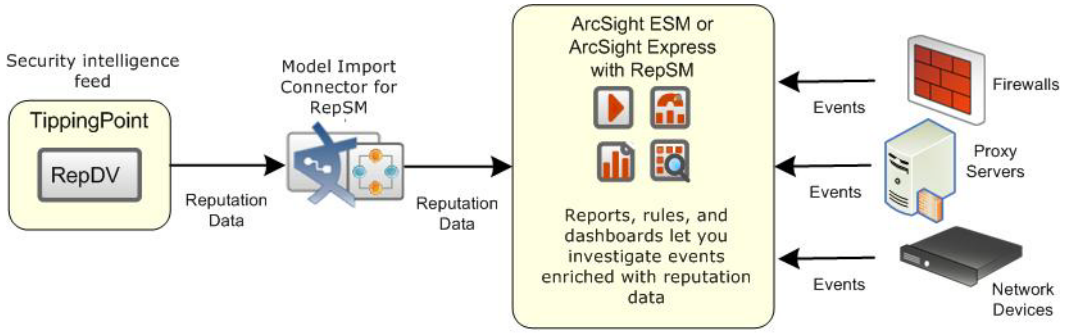
This chapter discusses the following topics:

How RepSM Works

The HP 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 HP RepSM service, powered by HP 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 HP Model Import Connector for RepSM imports the reputation data at regular intervals from the RepSM service to ArcSight ESM or ArcSight Express.
- The HP RepSM content running on ArcSight ESM or ArcSight 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.



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.

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:

Blended Threat	The malicious host is classified as having multiple exploit types.
Botnet	The malicious host is either a member of a botnet or a command and control center for a botnet.
Malware	The malicious host is one of the following: • A web server that distributes malware to users who browse sites located on the server. • A command and control center for computers infected with malware.
Miscellaneous	The host is considered malicious, but there is insufficient information to classify it as another, more specific exploit type.
Misuse and Abuse	The malicious host scans the internet for vulnerable systems, or serves adult content.
P2P	The malicious host is part of a peer-to-peer (P2P) network, such as eMule or BitTorrent. The malicious host might be the central node for the network or a member of the network.
Phishing	The malicious host sends phishing emails, or the malicious host's URL appears in the text of phishing emails.
Spam	The malicious host sends spam emails.
Spyware	The malicious host distributes spyware or other suspicious software.
Web Application Attacker	The malicious host initiates application layer attacks, such as SQL injection and Cross Site Scripting, against web servers.
Worm	The malicious host is infected by a worm.

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)

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.
- Analyze the past activity of infected computers for forensic investigation.

The **Internal Infected Assets** use case provides resources to perform these activities. For more information, see "Internal Infected Assets" on page 32.

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 37.

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 45.

Identify Suspicious Browsing

The **Access to Dangerous Destinations** use case detects users browsing to dangerous web sites and provides tools for investigating their activity. Operators can then take remedial action, such as using Threat Response Manager (TRM) to quarantine the user's computer. For more information about the use case, see "Access to Dangerous Destinations" on page 56.

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 49.

RepSM Detection Use Cases at a Glance

The following table summarizes some key points about the RepSM use cases that use threat intelligence to detect problems. This summary can help you understand the distinction between the use cases.

Use Case Name	Direction of Communication	Outcome of Communication	Malicious Host Exploit Type	The Use Case Detects Assets that are:
Internal Infected Assets	Outbound to malicious host	Success and failure	Botnet, P2P	**not** categorized as Public-Facing[a]
			All exploit types[b]	categorized as Public-Facing
Zero Day Attacks	Inbound from malicious host	Success	Botnet, Miscellaneous, Misuse and Abuse, P2P, Web Application Attacker, Worm	categorized as Internal Non Public-Facing
Dangerous Browsing	Outbound to malicious host	Success and failure	Phishing, Malware	**not** categorized as Public-Facing[a]
Access to Dangerous Destinations	Outbound to malicious host	Success and failure	Blended Threat, Miscellaneous, Misuse and Abuse, Spam, Spyware, Web Application Attacker, Worm	**not** categorized as Public-Facing[a]
Access from Dangerous Sources	Inbound from malicious host	Success	Blended Threat, Malware, Phishing, Spam, Spyware	categorized as Internal Non Public-Facing
			All exploit types[b]	**not** categorized as Internal Non Public-Facing[a]

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 8.

For detailed information about these and other RepSM use cases, see Chapter 3, Using RepSM Content, on page 25.

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 (IPSs)
- 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

Perform the installation tasks in the following order:

1. Verify your ArcSight ESM or ArcSight Express environment. See "Verifying Your Environment" on page 14.
2. For ArcSight ESM, increase the maximum capacity for active lists. See "Configuring the ESM Active List Capacity (Required)" on page 14.

   For ArcSight Express, this step is not required; the default active list capacity supports RepSM.
3. For ArcSight ESM, install the content package (`.arb` file). See "Installing the RepSM Content" on page 15.

   For ArcSight Express, this step is not required; the RepSM content package is pre-installed.
4. Install the Model Import Connector for RepSM. See "Installing the Model Import Connector for RepSM" on page 18.
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 18.

Verifying Your Environment

Before you install RepSM, make sure that you are running a supported version of ArcSight ESM or ArcSight Express. The *Reputation Security Monitor 1.01 Release Notes* indicate the supported versions.

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 ESM Active List Capacity (Required)

For ArcSight Express, the RepSM content package is pre-installed and the default active list capacity is one million; skip this section and go to "Installing the Model Import Connector for RepSM" on page 18 and then "Configuring the RepSM Content" on page 18. Some basic configuration is required or recommended to tailor the content for your operating environment.

By default, the maximum capacity for ArcSight ESM active lists is 500,000 entries. Before you install the RepSM content, this capacity must be increased to 1,000,000 to enable RepSM to monitor up to one million entries of reputation data. Otherwise, the installation of the RepSM content package will fail with the following error:

```
Install Failed: ActiveList capacity cannot be greater than 500000
```

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=1000000
   ```

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 *ESM Administrator's Guide*.

Installing the RepSM Content

> **Note**
> For ArcSight Express, the RepSM content package is pre-installed; skip this section and go to "Installing the Model Import Connector for RepSM" on page 18 and then "Configuring the RepSM Content" on page 18. Some basic configuration is required or recommended to tailor the content for your operating environment.

> **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, HP recommends that you back up any existing solutions installed on the ArcSight Manager. For detailed instructions, see Appendix B, Uninstalling RepSM, on page 71.

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

To install the RepSM content package:

1. Make sure the maximum capacity for active lists is set to 1,000,000, as described in "Configuring the ESM 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.1.0.0<nnnn>.0.arb`

   Where `<nnnn>` is the 4 character build number specified in the *Reputation Security Monitor 1.01 Release Notes*.

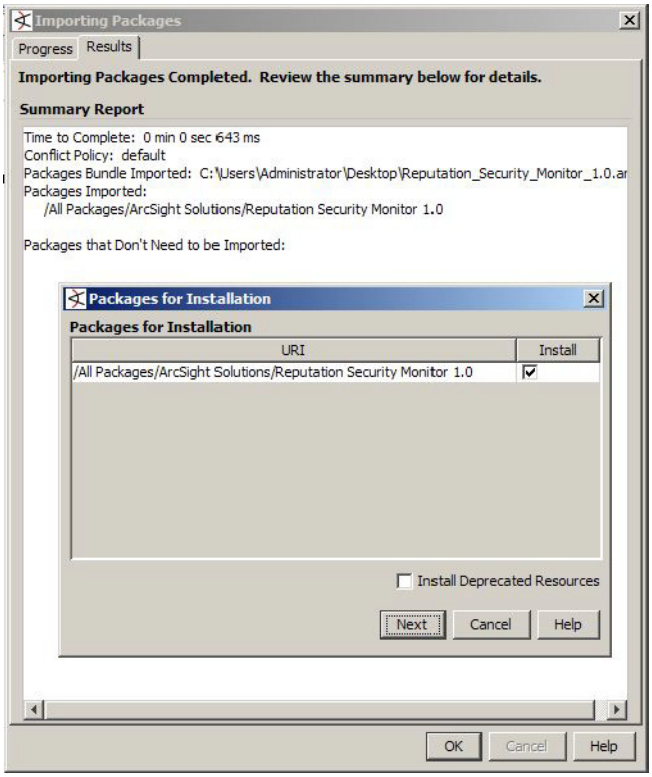
   > **Note**
   > Internet Explorer sometimes converts the ARB file to a ZIP file during download. If this occurs, rename the ZIP file back to an ARB file before importing.

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 1.0` checkbox selected and click **Next**.

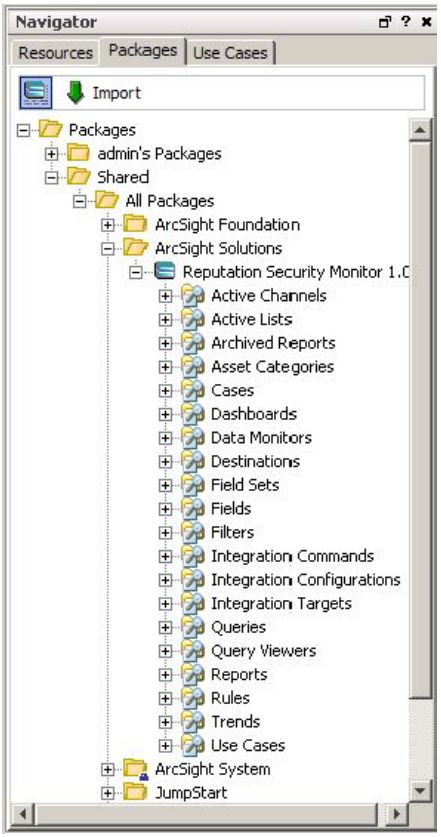
The Installing Packages dialog opens. The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the Summary Report.

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 1.0` group to verify that the installation is successful and that the content

is accessible in the Navigator panel.



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 18.

Troubleshooting Your Installation

If the installation is not successful, refer to the contact information below.

Resource	Description
Support web site	http://support.openview.hp.com provides access to incident reporting, the knowledge base, software downloads, help, and the customer forum.

Resource	Description
Protect 724 Community	https://protect724.arcsight.com offers a place for customers to: • Share content, collaborate on best practices, and get feedback • Ask and answer questions • Network with each other • Find product roadmaps • Sign up to receive email notifications about RepSM service outages from the RepSM group

For additional, post-installation troubleshooting information, see Appendix A, Troubleshooting, on page 67.

If you need to back up or uninstall the RepSM content at a later date, see Appendix B, Uninstalling RepSM, on page 71.

Installing the Model Import Connector for RepSM

The Model Import Connector for RepSM forwards reputation data from the RepSM service to ArcSight ESM or ArcSight 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 HP 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 1.01 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 25.

- "Assigning User Permissions" on page 19
- "Configuring Active Lists" on page 19
- "Categorizing Assets" on page 20
- "Deploying Rules (Required)" on page 21
- "Setting Thresholds for the Reputation Score" on page 22
- "Configuring Cases" on page 23
- "Verifying RepSM Content Configuration" on page 24

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 solution 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
- 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 1.0`.
   b. Right-click the **Reputation Security Monitor 1.0** 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**.

Configuring Active Lists

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.

Required Configuration

The following active lists require configuration to ensure that the use case produces results:

Active List	Used by this Use Case
Internal Domains for Reputation Monitoring Internal Network Addresses for Reputation Monitoring Internal Assets for Reputation Monitoring	"Internal Assets Found in Reputation Data" on page 45

Optional Configuration

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

Active List	Used by this Use Case
Critical Exploit Types	"Internal Infected Assets" on page 32
Dangerous Browsing Exploit Types	"Dangerous Browsing" on page 41
Zero Day Attack Exploit Types	"Zero Day Attacks" on page 37

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 8.

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

Categorizing Assets

Categorizing assets adds valuable business 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). By default, any address contained in the Private Address Space Zones is categorized as Protected.	`Site Asset Categories/Address Spaces`
Public-Facing	This RepSM asset category classifies internal assets that are accessible from the internet.	`ArcSight Solutions/Reputation Security Monitor`
Internal Non Public-Facing	This RepSM asset category classifies internal assets that are not accessible from the internet.	`ArcSight Solutions/Reputation 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:
"Access from Dangerous Sources" on page 52	Internal Non Public-Facing	Recommended
"Access to Dangerous Destinations" on page 56	Public-Facing	Recommended
"Dangerous Browsing" on page 41	Public-Facing	Recommended
"Internal Infected Assets" on page 32	Public-Facing	Recommended
"Zero Day Attacks" on page 37	Internal Non Public-Facing	Required

For more information about how categorization affects the use cases, see "RepSM Detection Use Cases at a Glance" 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 (Required)

In order for the RepSM rules to process events, the rules must be deployed to the `Real-time Rules` group. By default, RepSM rules are not deployed.

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

1. From the Resources tab in the Navigator panel, go to Rules and navigate to the `ArcSight Solutions/Reputation Security Monitor 1.0` group.
2. Right-click the `Reputation Security Monitor 1.0` 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 1.0` group.

   The rules in this group are linked to the rules in the `ArcSight Solutions/Reputation Security Monitor 1.0` group.

For more information about working with rules, see the ArcSight Console online Help.

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
Access from Dangerous Sources Reputation Domain Score Threshold Access from Dangerous Sources Reputation IP Score Threshold	"Access from Dangerous Sources" on page 52
Access to Dangerous Destinations Reputation Domain Score Threshold Access to Dangerous Destinations Reputation IP Score Threshold	"Access to Dangerous Destinations" on page 56
Dangerous Browsing Reputation Domain Score Threshold Dangerous Browsing Reputation IP Score Threshold	"Dangerous Browsing" on page 41
Internal Infected Assets Reputation Domain Score Threshold Internal Infected Assets Reputation IP Score Threshold	"Internal Infected Assets" on page 32
Zero Day Attacks Reputation Domain Score Threshold Zero Day Attacks Reputation IP Score Threshold	"Zero Day Attacks" on page 37

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.

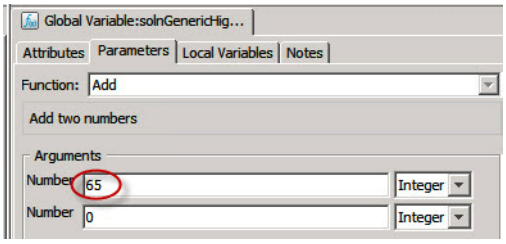
To set the threshold in the generic variable:

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:

   `Field Sets/Shared/All Field Sets/ArcSight Solutions/Reputation Security Monitor 1.0/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:

`Field Sets/Shared/All Field Sets/ArcSight Solutions/Reputation Security Monitor 1.0/Configuration`

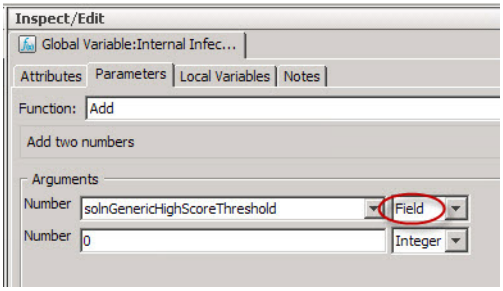
2 Double-click the variable to open it in the Inspect/Edit panel. (The variables are listed Table 2-1 on page 22.)

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.

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 1.0` group, which holds the cases generated by some RepSM rules.

You can add more groups to the `ArcSight Solutions/Reputation Security Monitor 1.0` 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 27.

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 60.

Chapter 3

Using RepSM Content

RepSM provides the use cases listed in the following table. For a detailed comparison of some of the use cases, see "RepSM Detection Use Cases at a Glance" on page 10.

Use Case	Purpose of Use Case
"RepSM Overview" on page 29	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.
"Internal Infected Assets" on page 32	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.
"Zero Day Attacks" on page 37	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, P2P, Web Application Attacker, and Worm. The exploit types are configurable, as described in "Configuration" on page 37.
"Dangerous Browsing" on page 41	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.
"Internal Assets Found in Reputation Data" on page 45	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.
"Event Enrichment with Reputation Data" on page 49	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.

Use Case	Purpose of Use Case
"Access from Dangerous Sources" on page 52	The Access from Dangerous Sources use case detects successful inbound communications to non-public facing internal assets from malicious entities that have an exploit type of Blended Threat, Malware, Phishing, Spam, or Spyware.
"Access to Dangerous Destinations" on page 56	The Access to Dangerous Destinations use case detects outbound communication to hosts that are involved in illegitimate activity such as sending spam or hosting spyware. Such communication can indicate either risky behavior on the part of users, or the existence of malware in the network. Although this type of communication is not as critical as communication with botnets and command and control centers, it can threaten the security of the network or harm the organization's reputation, and should be investigated to determine the root cause.

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

Use Case	Purpose of Use Case
"RepSM Package Health Status" on page 60	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.
"Reputation Data Analysis" on page 63	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, HP 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 1.0
```

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
- Access to Dangerous Destinations

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.

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.

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:

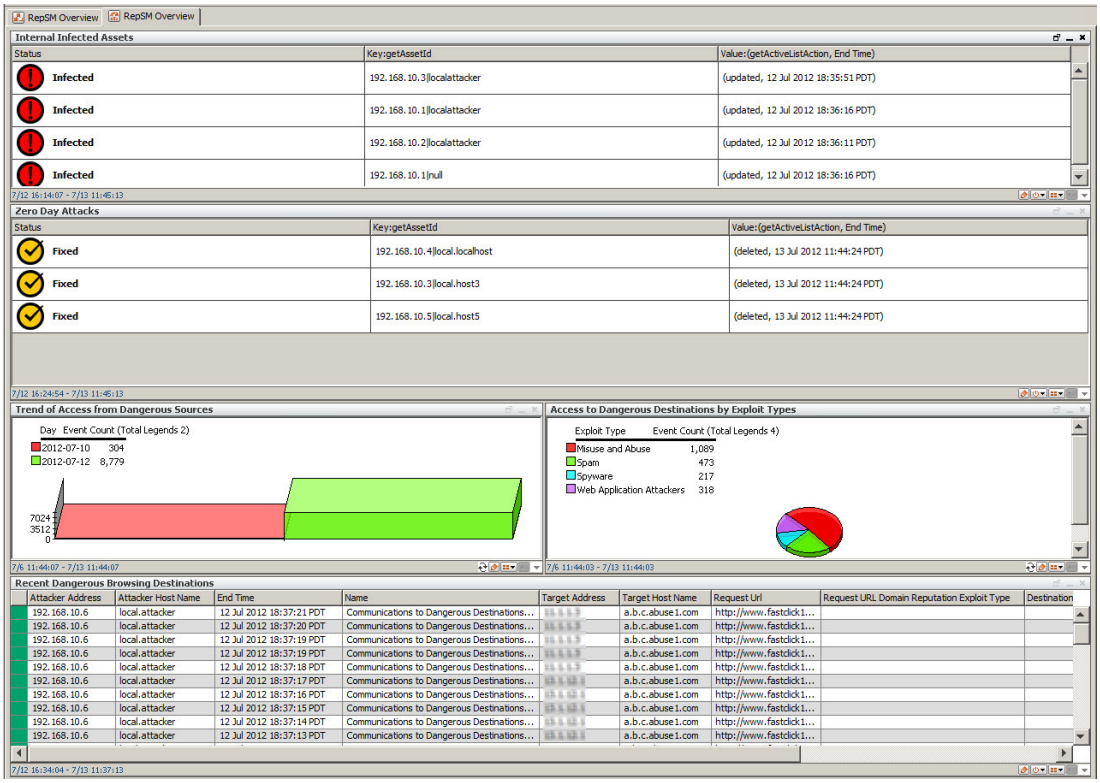
1. Click the **Use Cases** tab in the Navigator panel and open the **RepSM Overview** use case located in:

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation
   Security Monitor 1.0
   ```

2. Open the RepSM Overview dashboard.

   The dashboard provides a high-level, consolidated view of the RepSM use cases that detect issues based on threat intelligence:

   - Internal Infected Assets
   - Zero Day Attacks
   - Access from Dangerous Sources
   - Access to Dangerous Destinations
   - Dangerous Browsing

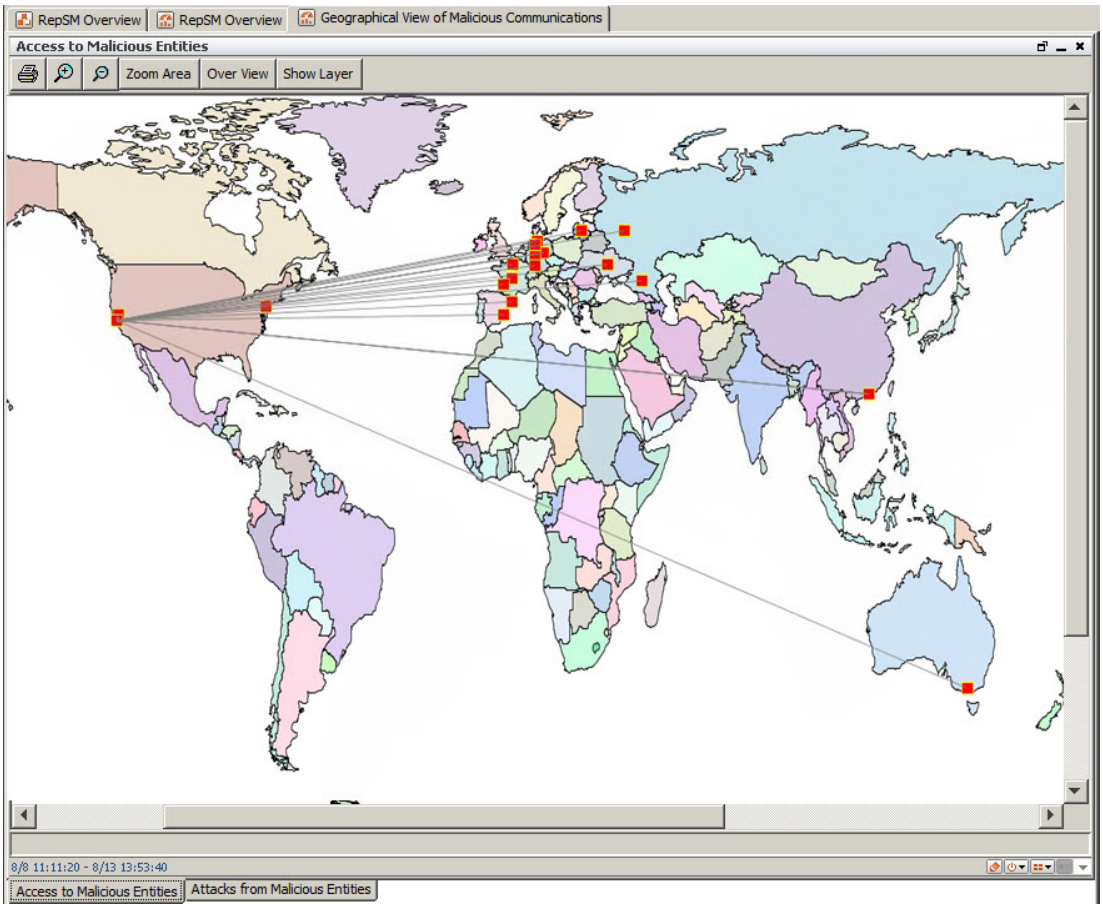


By using drilldowns, you can move from this dashboard to other use case dashboards for increasingly detailed information—including exploit types, reputation scores, detection times, attack counts, and event counts—and then finally to the base events that caused an asset to appear on the dashboard.

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 123.

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 9.

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 or P2P. These assets might be participating in a botnet or peer-to-peer network.

The exploit types are configurable, as described in "Configuration" on page 32.

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 27.

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 20.

- 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 and P2P. These exploit types are 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 8.

  For details about adding entries to an active list, see "Configuring Active Lists" on page 19.

- 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 22.

Usage

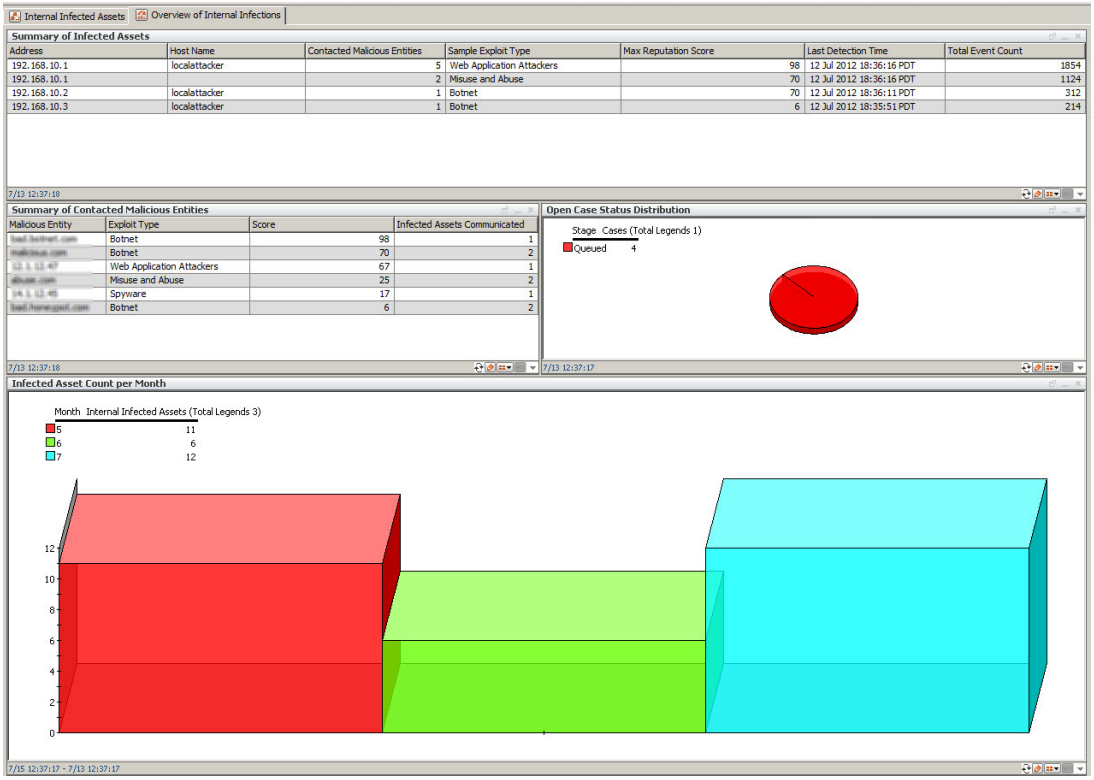
This section describes a likely scenario for investigating internal infected assets and highlights some key features of the use case.

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 1.0`

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 drilldown to:

- the base events that represent direct communication with a malicious entity
- other internal assets that might have been infected by the infected asset

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

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

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

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

The Summary of Contacted Malicious Entities component focuses on command and control centers that the internal asset contacted. Double-click a malicious entity to see which assets have communicated with it and then use the drilldowns to continue your investigation, as described in Step 5 and Step 7.

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

For more information about cases, see "Manage Cases to Ensure Continued Detection" on page 27.

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

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

Key Resources

The following 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 115.

Table 3-1 Resources that Support the Internal Infected Assets Use Case

Resource	Description	Type	URI
Monitor Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected 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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infection 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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infection Assets/`
Library Resources			
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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, P2P, Web Application Attacker, and Worm. The exploit types are configurable, as described in "Configuration" on page 37.

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 27.

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 20.

- 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, P2P, 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 8.

  For details about adding entries to an active list, see "Configuring Active Lists" on page 19.

- 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 22.

Usage

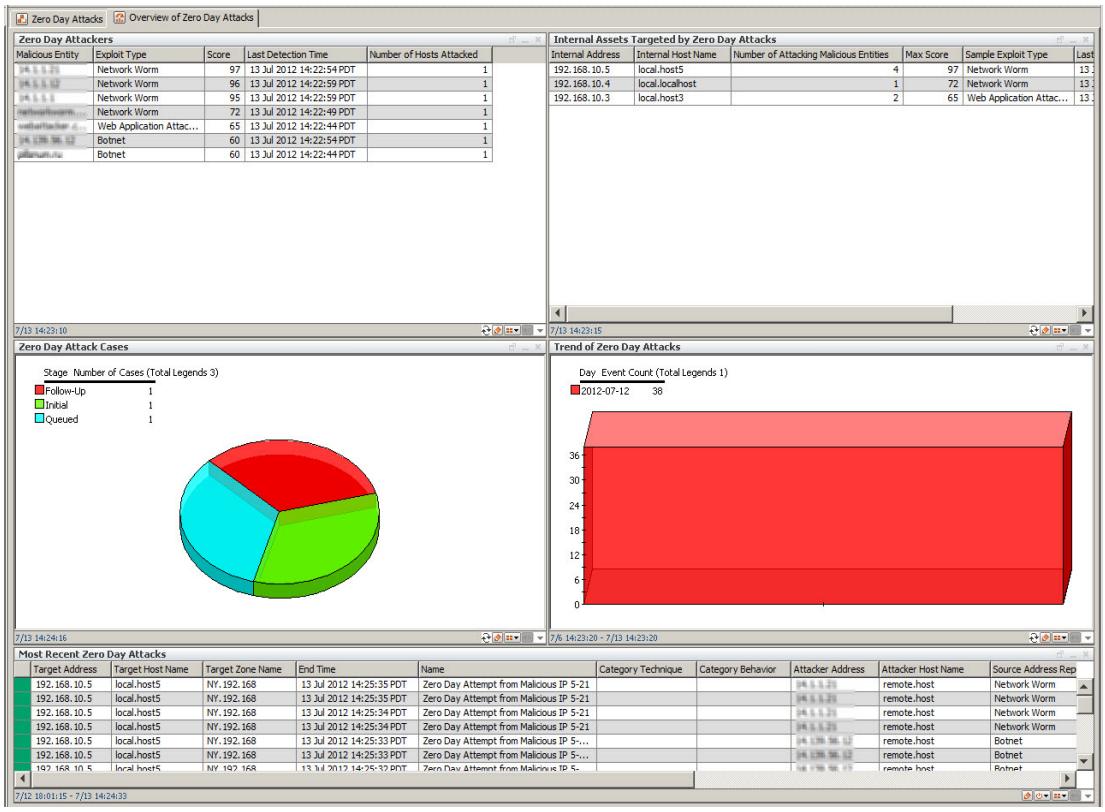
This section describes a likely scenario for investigating zero day attacks and highlights some key features of the use case.

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 1.0
   ```

   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 27.

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 156.

Table 3-2 Resources that Support the Zero Day Attacks Use Case

Resource	Description	Type	URI
Monitor Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`
Library Resources			
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant for zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, Miscellaneous.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`

Resource	Description	Type	URI
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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 "Configuration" on page 41.

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.

  This categorization is used by both the Dangerous Browsing use case and the Access to Dangerous Destinations use case.

  For more information, see "Categorizing Assets" 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:

  - Dangerous Browsing Reputation IP Score Threshold
  - Dangerous Browsing Reputation Domain Score Threshold

  For details, see "Setting Thresholds for the Reputation Score" on page 22.

- 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 8.

  For details about adding entries to an active list, see "Configuring Active Lists" on page 19.

Usage

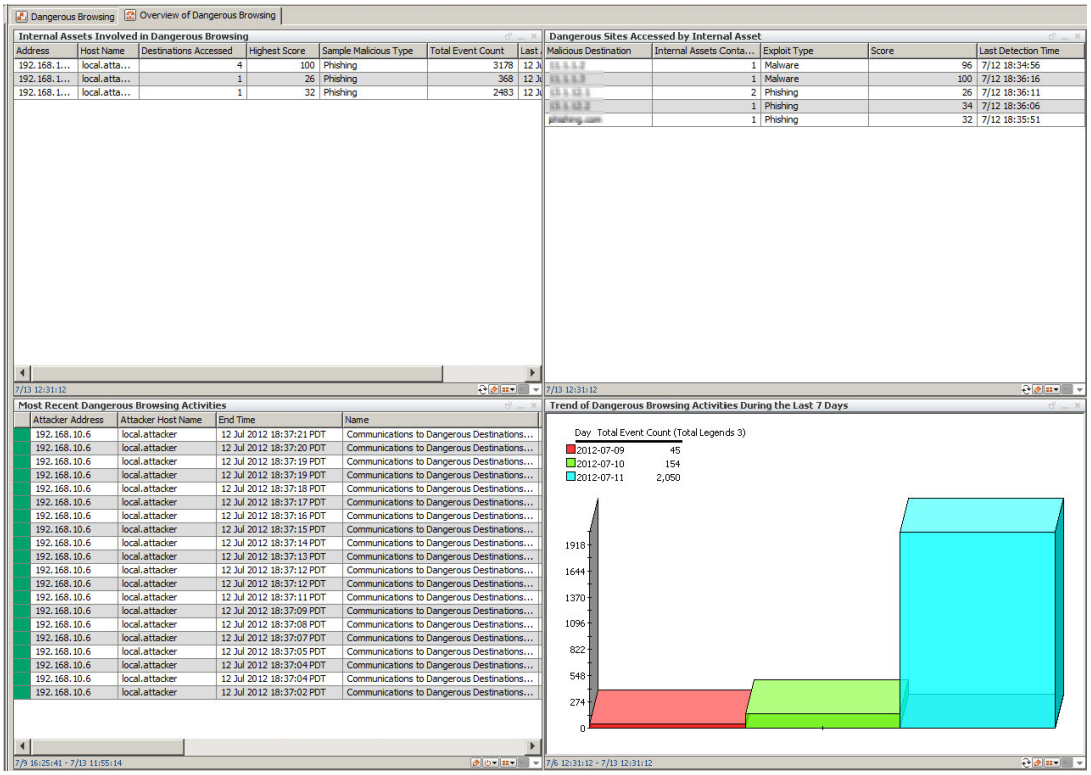
This section describes a likely scenario for investigating users browsing to dangerous web sties and highlights some key features of the use case.

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 1.0`

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 97.

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

Resource	Description	Type	URI
Monitor Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Dangerous Browsing Activities - One Year Trend	This report provides information about dangerous browsing activities by internal assets during the last year.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Dangerous Browsing Activities During the Last 7 Days	This report provides information about dangerous browsing activities by internal assets during the last 7 days.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Library Resources			

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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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 27.

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, hp.com or hp.co.uk.

    For details, see "Configuring Active Lists" on page 19.

- 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

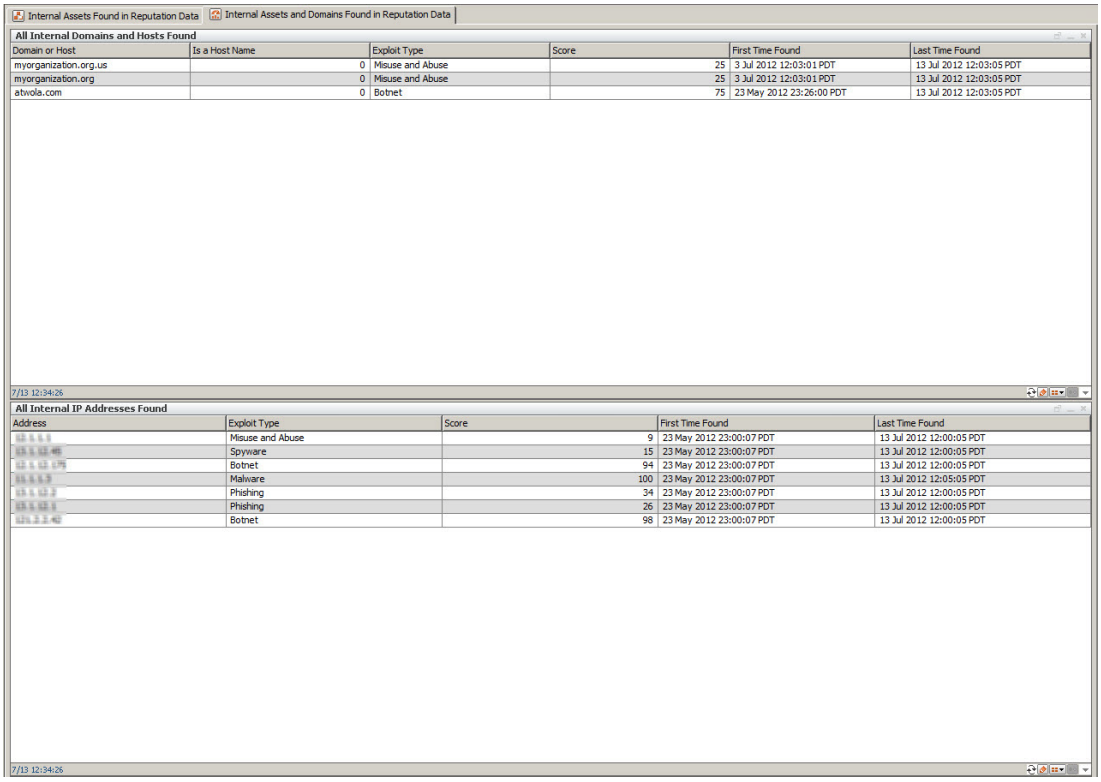
This section highlights some key features of the use case.

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 1.0`

   Review the resources provided by the use case.

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



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 27.

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 113.

Table 3-4 Resources that Support the Internal Assets Found in Reputation Data Use Case

Resource	Description	Type	URI
Monitor Resources			
Internal Assets and Domains Found in Reputation Data	This dashboard provides information around internal assets or domain names reported in the reputation database.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/`
Library Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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 hp.com or hp.co.uk.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitoring 1.0/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	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 special 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 3-5 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 3-5.

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 108.

Table 3-5 Resources that Support the Event Enrichment with Reputation Data Use Case

Resource	Description	Type	URI
Library Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/`

Resource	Description	Type	URI
Source Domain Reputation Score	This variable returns the reputation score of a malicious attacker (or a source) host name based on the reputation domain data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
Destination Address Reputation Score	This variable returns the reputation score of a malicious target (or a destination) host name based on the reputation IP data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
Reputation Domain Enrichment	This field set contains fields with reputation domain information for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Reputation IP Enrichment	This field set contains fields with reputation IP information for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Request URL Enrichment	This field set contains fields with reputation information (based on the request URL) for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Events with Requests to Malicious Hosts	This filter identifies events with requests to hosts found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/
Events from Malicious Sources	This filter identifies events whose attackers are found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/
Events to Malicious Targets	This filter identifies events whose targets are found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/

Access from Dangerous Sources

The Access from Dangerous Sources use case detects successful inbound communications to non-public facing internal assets from malicious entities that have an exploit type of Blended Threat, Malware, Phishing, Spam, or Spyware.

This use case does not open any cases.

Configuration

Configure the Access from Dangerous Sources use case as follows for your environment:

- Optional, but recommended. 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 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:

  - Access from Dangerous Sources Reputation Domain Score Threshold
  - Access from Dangerous Sources Reputation IP Score Threshold

  For details, see "Setting Thresholds for the Reputation Score" on page 22.

Usage

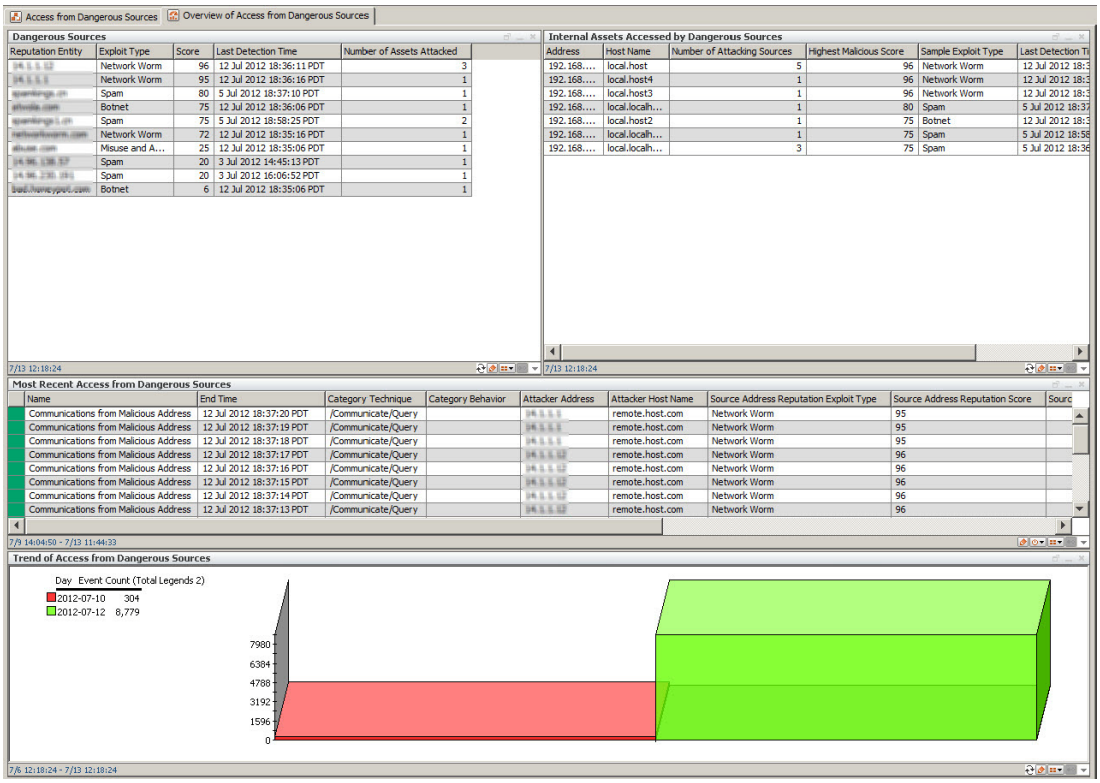
This section describes a likely scenario for investigating access from dangerous sources and highlights some key features of the use case.

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

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation
   Security Monitor 1.0
   ```

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

2 Open the Overview of Access from Dangerous Sources dashboard. Each component on the dashboard provides a different aspect of access from dangerous sources.



3 Review the information in the Internal Assets Accessed by Dangerous Sources on the dashboard. The internal assets in this list are assumed to have been contacted by dangerous sources and should be investigated immediately.

4 Double-click an asset to display additional information about the malicious entities that have communicated with the asset.

5 In the resulting display, double-click an asset to display the events associated with the infected asset.

6 In the resulting display, right-click a row and select **Investigate > Show 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 Dangerous Sources component to begin your investigation with the malicious entities, instead of the internal assets. Double-click a malicious entity to see which assets it has communicated with and then use the drilldowns to continue your investigation.

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 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 "Access from Dangerous Sources" on page 77.

Table 3-6 Resources that Support the Access from Dangerous Sources Use Case

Resource	Description	Type	URI
Monitor Resources			
Overview of Access from Dangerous Sources	This dashboard provides an overview of successful access from dangerous sources to internal, non public-facing assets. You can drilldown to see the base events related to the hosts involved.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Access from Dangerous Sources During the Last 24 Hours	This report shows data about access from dangerous sources to non public-facing, internal assets during the last 24 hours.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Access from Dangerous Sources - 30 Day Trend	This report shows data about access from dangerous malicious entities to non public-facing, internal assets during the last 30 days. Do not change the default value for the custom parameter AttackType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Access from Dangerous Sources - One Year Trend	This report shows data about access from dangerous sources to internal assets during the last year. Do not change the default value for the custom parameter AttackType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Access from Dangerous Sources During the Last 7 Days	This report shows data about access from dangerous sources to non public-facing, internal assets during the last seven days. Do not change the default value for the custom parameter AttackType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Library Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`

Access to Dangerous Destinations

The Access to Dangerous Destinations use case detects outbound communication to hosts that are involved in illegitimate activity such as sending spam or hosting spyware. Such communication can indicate either risky behavior on the part of users, or the existence of malware in the network. Although this type of communication is not as critical as communication with botnets and command and control centers, it can threaten the security of the network or harm the organization's reputation, and should be investigated to determine the root cause.

This use case detects outbound communication from internal assets, which are not public-facing, to malicious hosts that have an exploit type of Blended Threat, Miscellaneous, Misuse and Abuse, Spam, Spyware, Web Application Attacker, or Worm.

This use case does not open any cases.

Configuration

Configure the Access to Dangerous Destinations 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 provides a better context for the detected events and helps reduces false positives.

  This categorization is used by both the Dangerous Browsing use case and the Access to Dangerous Destinations use case.

  For more information, see "Categorizing Assets" 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:

  - Access to Dangerous Destinations Reputation Domain Score Threshold
  - Access to Dangerous Destinations Reputation IP Score Threshold

  For details, see "Setting Thresholds for the Reputation Score" on page 22.

Usage

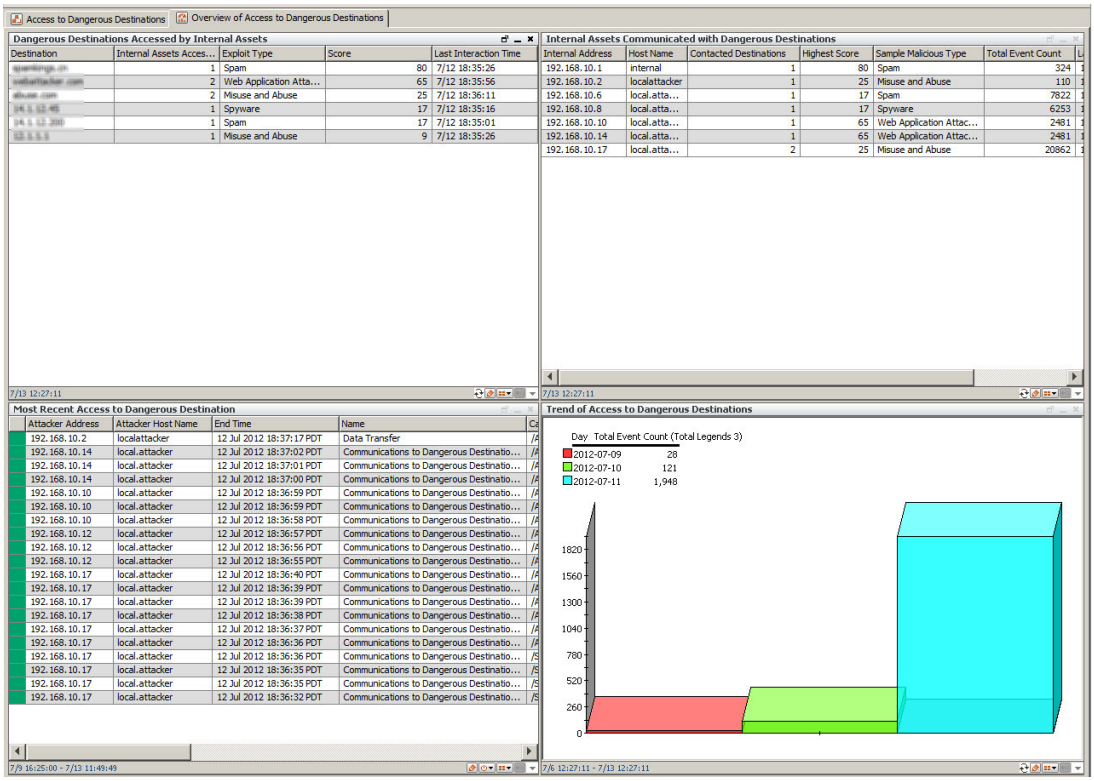
This section describes a likely scenario for investigating access to dangerous destinations and highlights some key features of the use case.

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

   ```
   Use Cases/Shared/All Use Cases/ArcSight Solutions/Reputation
   Security Monitor 1.0
   ```

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

2 Open the Overview of Access to Dangerous Destinations dashboard.



3 In the Internal Assets Communicated with Dangerous Destinations component, double-click an internal asset to display the dangerous destinations it has contacted.

4 In the resulting display, double-click an internal asset to display the correlation events for that asset.

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

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

The Dangerous Destinations Accessed by Internal Assets component enables you to start your investigation with the malicious entity and drilldown to the assets that contacted it, and then to the events involving them.

7 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 access to dangerous destinations.

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 "Access to Dangerous Destinations" on page 86.

Table 3-7 Resources that Support the Access to Dangerous Destinations Use Case

Resource	Description	Type	URI
Monitor Resources			
Overview of Access to Dangerous Destinations	This dashboard shows an overview of all access to dangerous destinations. You can drilldown to more information about the related destinations and the correlation or base events.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations - One Year Trend	This report provides information about access to dangerous destinations by internal assets during the last year. It uses the same queries as the counterpart report for dangerous browsing activities, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations During the Last 24 Hours - Short Form	This report provides information about access to dangerous destinations, which have exploit types that are not defined in the Dangerous Browsing Exploit Types active list, by internal assets during the last 24 hours. It contains less information than the long counterpart.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations - 30 Day Trend	This report provides information about access to dangerous destinations by internal assets during the last 30 days. It uses the same queries as the counterpart report for dangerous browsing activities, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations During the Last 24 Hours - Long Form	This report provides information about access to dangerous destinations of non-browsing exploit types by internal assets during the last 24 hours.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`

Resource	Description	Type	URI
Access to Dangerous Destinations During the Last 7 Days	This report provides information about access to dangerous destinations by internal assets during the last seven days. It uses the same queries as the counterpart report for dangerous browsing destinations, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Library Resources			
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`

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.

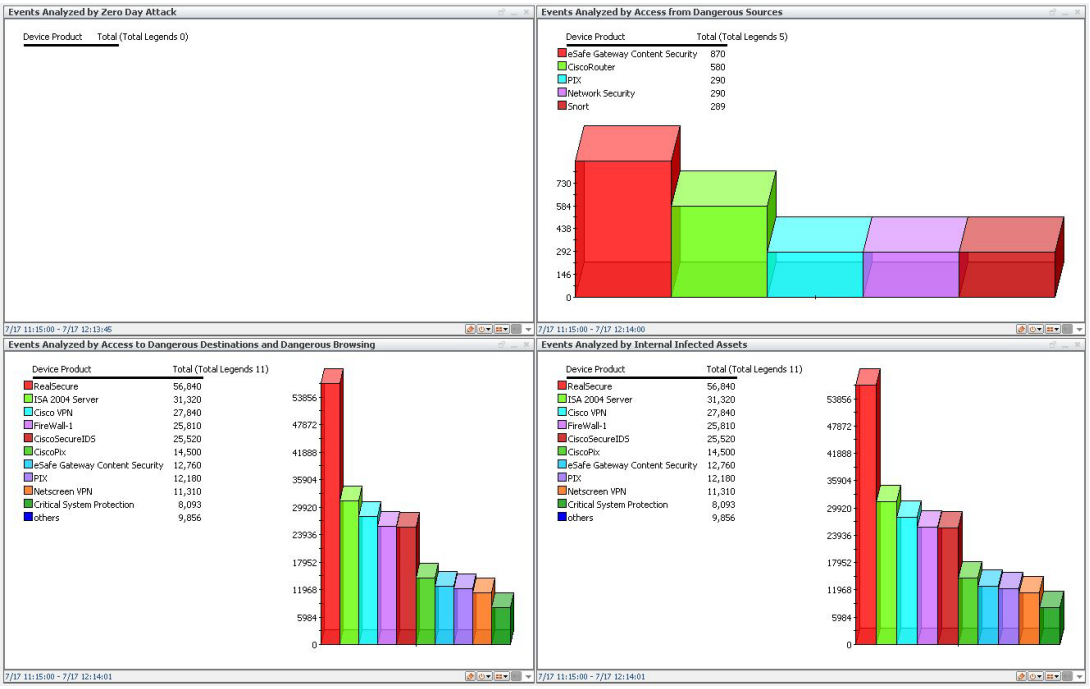
Usage

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 1.0`

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 67.

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, the cause should be investigated, 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 136.

Table 3-8 Resources that Support the RepSM Package Health Status Use Case

Resource	Description	Type	URI
Monitor Resources			
Inbound Events	This active channel shows events the RepSM package considers as inbound.	Active Channel	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/`
Outbound Events	This active channel shows events the RepSM package considers as outbound.	Active Channel	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/`
RepSM Rules Health	This dashboard provides an overview of rules in the RepSM package, including their status and logs.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/`

Resource	Description	Type	URI
Events Analyzed by RepSM Use Cases	This dashboard provides an overview of the traffic monitored for reputation data.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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.

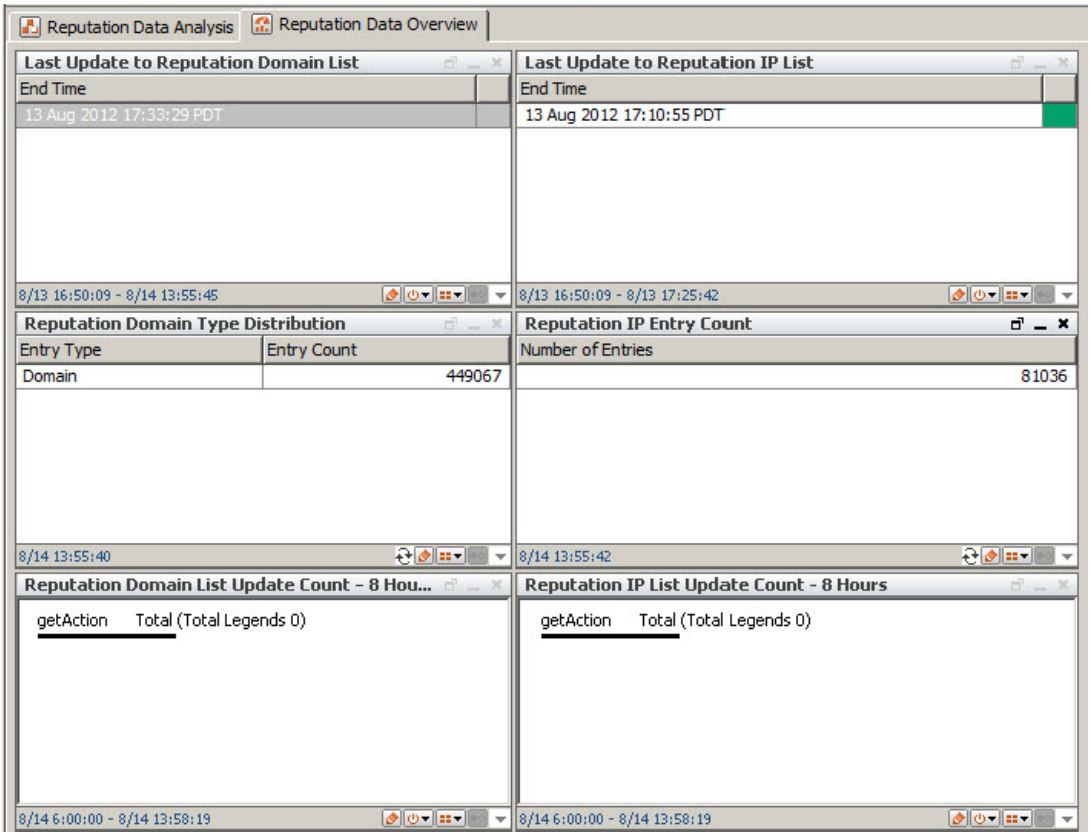
Usage

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 1.0`

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, respectively.

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 151.

Table 3-9 Resources that Support the Reputation Data Analysis Use Case

Resource	Description	Type	URI
Monitor Resources			
Reputation Domain Database Overview	This dashboard shows an overview of the reputation domain database (stored in an active list) in the system.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/`
Reputation IP Entries	This query viewer shows the top 1,000,000 IP entries in the reputation IP active list.	Query Viewer	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/`
Reputation Domain Entries	This query viewer shows the top 1,000,000 domain entries in the reputation domain active list.	Query Viewer	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/`

Resource	Description	Type	URI
Reputation Database Changes During the Last 1 Year - Exploit Type Specific	This report shows the changes of a specific reputation exploit type during the last year.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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
On ArcSight ESM, the installation of the RepSM content package fails with the following error: `Install Failed: ActiveList capacity cannot be greater than 500000`	Increase the active list maximum capacity, as described in "Configuring the ESM Active List Capacity (Required)" on page 14.
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.	In the following order: • Make sure the Model Import Connector for RepSM is running. • Make sure the Model Import Connector for RepSM is not out of memory. Look for an `OutOfMemoryError` message in the `$ARCSIGHT_HOME\current\logs\agent.log`. If necessary, increase the Model Import Connector for RepSM Java heap memory size to at least 2 GB, as described in the Model Import Connector for RepSM Configuration Guide. • Make sure the **Model Import User** 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. • Make sure the ArcSight Manager is collecting events from the devices described in "Supported Devices" on page 11. • Make sure the RepSM rules are deployed, as described in "Deploying Rules (Required)" on page 21. • Make sure the use case is configured properly. Several use cases require asset categorization or other configuration to capture events. For configuration details, see "Configuring the RepSM Content" on page 18 and Chapter 3, Using RepSM Content, on page 25. • Make sure inbound events are being sent to ArcSight Manager. Check the Inbound Events active channel. • Make sure outbound events are being sent to ArcSight Manager. Check the Outbound Events active channel. • Make sure the event source connector and ArcSight Manager are synchronized; the *Manager Receipt Time* should be no more than a few seconds later than the event *End Time*. Use the Inbound Events or Outbound Events active channel to open an event in the Event Inspector and compare these times.
The number of reputation data entries imported into the ArcSight Manager seems very low. There might also be reputation data archive files that have a file extension of `xml.bad` in `ARCSIGHT_HOME\archive\webservices`.	Make sure the following Model Import Connector for RepSM property is set in the `agent.properties` file located at `ARCSIGHT_HOME\current\user\agent`: `buildmodeldelay=60000` (one minute expressed in milliseconds) This property controls how frequently the archives are sent to the Manager. If it is set too low, the connector will send archives too frequently. For more information abou this property, see the Model Import Connector for RepSM Configuration Guide.

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

Problem	Solution
The RepSM use case dashboards do not show any *recent* activity; the data seems stale.	Check the Reputation Data Overview dashboard in the Reputation Data Analysis use case to see when the reputation data active lists were last updated. If the active lists have not been updated in the last 12 hours or so, there might be a problem with either the RepSM service or the Model Import Connector for RepSM. For example, the service might have expired or the connector might need to be restarted. To check the status of either component, open the RepSM Package Health Status use case and review the messages in the RepSM Resource Health dashboard. For an explanation of the service messages, see Appendix C, RepSM Service Messages, on page 75. If the messages do not reveal any obvious issues, search the connector log at `$ARCSIGHT_HOME\current\logs\agent.log` for network error messages, such as: • connection timeout • host cannot be reached and address those network issues. If there are no obvious network issues, look for an `OutOfMemoryError` message in the `$ARCSIGHT_HOME\current\logs\agent.log`. If necessary, increase the Model Import Connector for RepSM Java heap memory size to at least 2 GB, as described in the Model Import Connector for RepSM Configuration Guide. 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: https://protect724.arcsight.com/groups/repsm If you cannot determine cause of the problem, contact Customer Support.
The reputation data includes an entry for an IP address, host name, or domain name that is **not** malicious.	Delete 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 entry might reappear in the active lists. To remove the entry more permanently, gather the following information and contact Customer Support. • The IP address, host name, or domain name to be removed. • Any relevant event details (depending on the source of the event), such as the request URL, source port, destination port, and matching signature.
On ArcSight ESM, some dashboards display *numerical* 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.

Appendix B

Uninstalling RepSM

This chapter provides instructions on how to uninstall RepSM and discusses the following topics.

Preparing to Uninstall

Before you uninstall the RepSM content package, make sure you back up the content. Performing a backup ensures that the content is preserved. See "Backing Up a Solution Package" on page 72.

Optionally, before you back up the content, you can generate a list of the resource changes since the last time the package was exported to a package bundle. You can then back up only those resources that have been modified or added. See "Generating a List of Resource Changes" on page 71.

Generating a List of Resource Changes

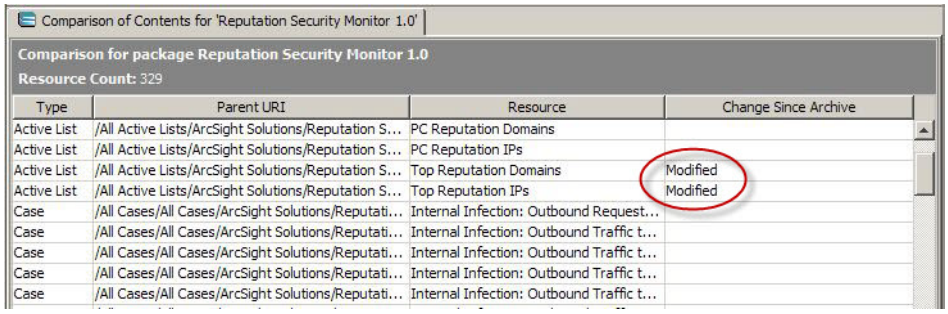
Before backing up and uninstalling a solution content package, you can generate a list of the resource changes since the last time the package was exported to a package bundle. The current resources associated with the selected package are compared against the resources saved in the package bundle and any new, modified or deleted resources are reported.

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

To generate a list of resource changes:

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` 1.01 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`.



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

Backing Up a Solution Package

HP 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 "Generating a List of Resource Changes" on page 71.

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 the solution group.

For RepSM, navigate to `ArcSight Solutions/`.

3 Right-click the package ( ) (such as `Reputation Security Monitor` 1.01) 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.

Uninstalling the Content Package

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. For detailed instructions, see Backing Up a Solution Package, above. To generate a list of resource changes before the uninstall, see "Generating a List of Resource Changes" on page 71.

To uninstall the content package:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. Click the **Packages** tab in the Navigator panel.
3. Navigate to `ArcSight Solutions`, right-click the `Reputation Security Monitor 1.0` package (), and select **Uninstall Package**.
4. 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 displays indicating that there is a conflict, select an option in the **Resolution Options** area and click **OK**.
5. When the uninstall is complete, review the summary and click **OK**.

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 HP. For more information, see the Model Import Connector for RepSM *Configuration Guide*. If the activation continues to fail, contact HP ArcSight Customer Support.
3:Trial period expired on *YYYY-MM-DDThh:mm:ssZ*	The activation of the RepSM service failed because the trial license expired on the date shown in the message.	Contact your HP ArcSight sales representative to obtain a new license.
4:Key expired on *YYYY-MM-DDThh:mm:ssZ*	The activation of the RepSM service failed because the activation key expired on the date shown in the message.	Contact your HP ArcSight sales representative to obtain a new activation key.
5:Service terminated on *YYYY-MM-DDThh:mm:ssZ*	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. If your organization did not request the termination, contact HP 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 *DD-MM-YYYYThh:mm:ss*	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. If your organization did not request the termination, contact HP ArcSight Customer Support.
5:Service will expire in *nn* 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:

For information about the key resources for each use case, see the "Key Resources" sections in Chapter 3, Using RepSM Content, on page 25. Key resources are those that you use during an investigation or that might require configuration.

Access from Dangerous Sources

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

Table D-1 Resources that Support the Access from Dangerous Sources Use Case

Resource	Description	Type	URI
Monitor Resources			
Overview of Access from Dangerous Sources	This dashboard provides an overview of successful access from dangerous sources to internal, non public-facing assets. You can drilldown to see the base events related to the hosts involved.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`

Resource	Description	Type	URI
Dangerous Sources	This query viewer shows the dangerous sources accessing internal, non public facing assets, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Internal Assets Accessed by Dangerous Sources	This query viewer shows the summary of internal assets accessed by dangerous sources, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected and the time of the latest attack.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Access from Dangerous Sources During the Last 24 Hours	This report shows data about access from dangerous sources to non public-facing, internal assets during the last 24 hours.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Access from Dangerous Sources - 30 Day Trend	This report shows data about access from dangerous malicious entities to non public-facing, internal assets during the last 30 days. Do not change the default value for the custom parameter AttackType.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Access from Dangerous Sources - One Year Trend	This report shows data about access from dangerous sources to internal assets during the last year. Do not change the default value for the custom parameter AttackType.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Access from Dangerous Sources During the Last 7 Days	This report shows data about access from dangerous sources to non public-facing, internal assets during the last seven days. Do not change the default value for the custom parameter AttackType.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Library - Correlation Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
Access from Dangerous Sources: Successful Inbound Communications from Malicious Domain	This rule captures the first event of all successful inbound communications to internal, non public-facing assets from reputation domain names with zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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 zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant for zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, Miscellaneous.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with Zero-Day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
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 7 days.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	ArcSight Solutions/Reputation Security Monitor
Most Recent Access from Dangerous Sources	This data monitor shows the last 20 access activities from dangerous sources to non public-facing internal assets.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerDomainExploitType	This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerDomainLevel2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerDomainLevel1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerReputationHostNameListEntry	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation 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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Zero Day Attack Reputation IP Exploit Types	This filter identifies events from malicious IP addresses having zero day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Non Public-Facing Internal Targets	This filter identifies all events whose targets are categorized as non public-facing internal.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Inbound Events	This filter identifies events coming from outside the network in your organization targeting the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Inbound Communication from Malicious Domains	This filter identifies all inbound traffic from domain names in the reputation domain active list.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Access from Dangerous Sources	This filter identifies all access from dangerous sources. By default, any successful inbound communication not flagged as zero-day attack is flagged as such.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Zero Day Attack Reputation Domain Exploit Types	This filter identifies events from malicious domain names or host names having zero-day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
Access from Dangerous Sources - Rule Firings	This filter identifies all correlation events generated by rules that detect access from dangerous sources.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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 7 days. It is based on a trend so it might not show most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/

Resource	Description	Type	URI
Zero Day Attacks per Reputation Type During the Last 30 Days	This query returns the number of zero day attacks per reputation (exploit) type within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Summary of Dangerous Sources	This query returns the dangerous sources accessing internal, non public facing assets, ordered by the highest score, the type of the attacker, the number of internal assets it attacked, and the last communication time.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/`
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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Summary of Internal Assets Accessed by Dangerous Sources	This query returns the summary of internal assets accessed by dangerous sources, including the number of attacking sources, the highest reputation score of these attackers, the total number of events detected and the time of the latest attack.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/`

Resource	Description	Type	URI
Top Assets Most Attacked During the Last 7 Days	This query returns the internal assets received most zero day attacks during the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Top Accessed Assets During the Last 24 Hours	This query returns the internal assets being accessed the most during the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/`
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	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
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 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Access from Dangerous Sources per Reputation Type During the Last 24 Hours	This query returns the count of access from dangerous sources per reputation (exploit) type within the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/`
Access from Dangerous Sources in the Last 24 Hours	This query returns all access from dangerous sources in the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/`
Zero Day Attack Details During the Last 7 Days	This query returns the details of zero day attacks within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Zero Day Attacks per Reputation Type During the Last One Year	This query returns the number of zero day attacks per reputation (exploit) type within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/`
Zero Day Attacks and Access from Dangerous Sources	This trend stores all firings of rules that detect zero day attacks or access from dangerous sources.	Trend	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`

Access to Dangerous Destinations

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

Table D-2 Resources that Support the Access to Dangerous Destinations Use Case

Resource	Description	Type	URI
Monitor Resources			
Overview of Access to Dangerous Destinations	This dashboard shows an overview of all access to dangerous destinations. You can drilldown to more information about the related destinations and the correlation or base events.	Dashboard	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Dangerous Destinations Accessed by Internal Assets	This query viewer shows the summary of dangerous destinations contacted by internal hosts.	Query Viewer	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Internal Assets Communicated with Dangerous Destinations	This query viewer shows the summary of internal assets that communicated with a dangerous destination.	Query Viewer	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`

Resource	Description	Type	URI
Trend of Access to Dangerous Destinations	This query viewer shows the top daily count of communications with dangerous destinations (domain, host name or IP address) during the last 7 days. It is based on a trend so it might not show most recent data.	Query Viewer	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations - One Year Trend	This report provides information about access to dangerous destinations by internal assets during the last year. It uses the same queries as the counterpart report for dangerous browsing activities, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations During the Last 24 Hours - Short Form	This report provides information about access to dangerous destinations, which have exploit types that are not defined in the Dangerous Browsing Exploit Types active list, by internal assets during the last 24 hours. It contains less information than the long counterpart.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations - 30 Day Trend	This report provides information about access to dangerous destinations by internal assets during the last 30 days. It uses the same queries as the counterpart report for dangerous browsing activities, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations During the Last 24 Hours - Long Form	This report provides information about access to dangerous destinations of non-browsing exploit types by internal assets during the last 24 hours.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access to Dangerous Destinations During the Last 7 Days	This report provides information about access to dangerous destinations by internal assets during the last seven days. It uses the same queries as the counterpart report for dangerous browsing destinations, but with a different activity type. Because of this, do not change the default value of the custom variable ActivityType.	Report	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Library - Correlation Resources			

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Dangerous Browsing: Outbound Requests to Malicious Domains	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Browsing: Outbound Communications to Malicious Domains	This rule captures all dangerous browsing activities from non public-facing assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Browsing: Outbound Communications to Malicious IPs	This rule captures all dangerous browsing activities from non public-facing assets to reputation IP addresses with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/

Resource	Description	Type	URI
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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 7 days.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Protected	This is a site asset category.	Asset Category	`Site Asset Categories/Address Spaces`
Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`
Most Recent Access to Dangerous Destination	This data monitor shows the last 20 access to dangerous destination activities from non public-facing internal assets.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/`

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
Destination Address Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) IP based on the reputation IP data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/

Resource	Description	Type	URI
solnGetTarget DomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationDo mainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetTarget DomainExploit Type	This variable returns the exploit type of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetLowerT argetHostNam e	This variable returns the target host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationHos tNameListEntr y	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTarget DomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTarget ReputationDo mainLevel2List Entry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetReques tURLReputatio nDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/

Resource	Description	Type	URI
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
Dangerous Browsing Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/

Resource	Description	Type	URI
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Interactions with Dangerous Destinations - Rule Firings	This filter identifies all firings of rules that detect interactions with dangerous destinations (i.e. non-browsing exploit types).	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Dangerous Destinations and Dangerous Browsing: Outbound Communicatio n 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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Access to Dangerous Destinations	This filter identifies all access to dangerous destinations.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Dangerous Browsing Target Reputation IP Exploit Types	This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Outbound Communication to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	Filter	`ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/`
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	Filter	`ArcSight Solutions/Reputation Security Monitor 1.0/General/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/`
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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Weekly Count of Dangerous Browsing Activities During the Last 30 Days	This query returns the number of dangerous browsing activities per week within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`

Resource	Description	Type	URI
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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Top Assets Interacted Most with Dangerous Destinations During the Last 24 Hours	This query returns the internal assets that interacted most with dangerous destinations (ie. of non-browsing exploit types) during the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Dangerous Destinations Accessed by Internal Assets	This query returns the summary of dangerous destinations contacted by internal hosts.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
Interactions with Dangerous Destinations in the Last 24 Hours	This query returns all interactions with dangerous destinations (non-browsing types only) in the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
Internal Assets Communicated with Dangerous Destinations	This query returns the summary of internal assets that communicated with a dangerous destination.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
Top 10 Dangerous Destinations Most Accessed During the Last 24 Hours	This query returns the top dangerous destinations (domain, host name or IP address) of non-browsing exploit types that were accessed the most during the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`

Resource	Description	Type	URI
Dangerous Browsing Activities per Reputation Type During the Last One Year	This query returns the number of dangerous browsing activities per reputation (exploit) type within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Daily Communications with Dangerous Destinations During the Last 7 Days	This query returns the top daily count of communications with dangerous destinations (domain, host name or IP address) during the last 7 days. It is based on a trend so it might not show most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Top 10 Dangerous Destinations Accessed by Most Internal Assets During the Last 24 Hours	This query returns the top dangerous destinations (domain, host name or IP address) of non-browsing types that have the highest number of internal assets interacted with during the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Dangerous Browsing Activities During the Last 7 Days	This query returns dangerous browsing activities within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`

Resource	Description	Type	URI
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 within the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/
Interactions with Dangerous Destinations per Reputation Type During the Last 24 Hours	This query returns the number of interactions to dangerous destinations (non-browsing types) per reputation (exploit) type within the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/
Monthly Count of Dangerous Browsing Activities During the Last One Year	This query returns the number of dangerous browsing activities per month within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/

Dangerous Browsing

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

Table D-3 Resources that Support the Dangerous Browsing Use Case

Resource	Description	Type	URI
Monitor Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/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 7 days. It is based on a trend so it might not show most recent data.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Internal Assets Involved in Dangerous Browsing	This query viewer shows the summary of internal assets involved in dangerous browsing.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Sites Accessed by Internal Asset	This query viewer shows the summary of dangerous web sites accessed by internal hosts.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Browsing Activities - One Year Trend	This report provides information about dangerous browsing activities by internal assets during the last year.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Browsing Activities During the Last 7 Days	This report provides information about dangerous browsing activities by internal assets during the last 7 days.	Report	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Library - Correlation Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Dangerous Browsing: Outbound Requests to Malicious Domains	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Dangerous Browsing: Outbound Communications to Malicious Domains	This rule captures all dangerous browsing activities from non public-facing assets to reputation domain names with high scores and non-critical exploit types.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Dangerous Browsing: Outbound Communications to Malicious IPs	This rule captures all dangerous browsing activities from non public-facing assets to reputation IP addresses with high scores and non-critical exploit types.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`

Resource	Description	Type	URI
Malicious Host Names in Dangerous Destination Interactions and Dangerous Browsing	This active list stores all malicious host names involved in interactions with dangerous destinations and dangerous sites. It is used internally to show all base events, and has a time-to-live of 7 days.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Protected	This is a site asset category.	Asset Category	`Site Asset Categories/Address Spaces`
Public-Facing	This is a solutions asset category.	Asset Category	`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	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`

Resource	Description	Type	URI
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
Destination Address Reputation Exploit Type	This variable returns the exploit type of a malicious target (or a destination) IP based on the reputation IP data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/

Resource	Description	Type	URI
solnGetTarget ReputationDo mainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetTarget DomainExploit Type	This variable returns the exploit type of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetLowerT argetHostNam e	This variable returns the target host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationHos tNameListEntr y	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTarget DomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTarget ReputationDo mainLevel2List Entry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetReques tURLReputatio nDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTarget ReputationDo mainLevel3List Entry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
Dangerous Browsing Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Dangerous Browsing Activities - Rule Firings	This filter identifies all firings of rules that detect dangerous browsing activities.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/

Resource	Description	Type	URI
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Interactions with Dangerous Destinations - Rule Firings	This filter identifies all firings of rules that detect interactions with dangerous destinations (i.e. non-browsing exploit types).	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Dangerous Browsing	This filter identifies all dangerous browsing activities.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Dangerous Browsing Target Reputation IP Exploit Types	This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Outbound Communication to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
Dangerous Browsing Activities in the Last 24 Hours	This query returns all dangerous browsing activities in the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/
Top Assets with Most Dangerous Browsing Activities During the Last 7 Days	This query returns the internal assets with most browsing activities during the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/

Resource	Description	Type	URI
Weekly Count of Dangerous Browsing Activities During the Last 30 Days	This query returns the number of dangerous browsing activities per week within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Daily Dangerous Browsing Activities During the Last 7 Days	This query returns the top daily count of dangerous activities during the last 7 days. It is based on a trend so it might not show most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 (ie. of non-browsing exploit types) during the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
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 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Dangerous Browsing Activities During the Last 7 Days	This query returns dangerous browsing activities within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 30 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Dangerous Browsing Activities per Reputation Type During the Last 24 Hours	This query returns the number of dangerous browsing activities per reputation (exploit) type within the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`
Dangerous Browsing and Interactions with Dangerous Destinations - Trend Base	This query returns all firings of rules that detect dangerous browsing or access to dangerous destinations within the last 24 hours.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/`
Monthly Count of Dangerous Browsing Activities During the Last One Year	This query returns the number of dangerous browsing activities per month within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/Dangerous Browsing/`

Resource	Description	Type	URI
Dangerous Browsing Activities per Reputation Type During the Last 7 Days	This query returns the number of dangerous browsing activities per reputation (exploit) type within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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-4 Resources that Support the Event Enrichment with Reputation Data Use Case

Resource	Description	Type	URI
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/`
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/`

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	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLReputationDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
Request URL Reputation Domain	This variable returns the reputation domain from a URL request based on the reputation domain data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
Destination Address Reputation Score	This variable returns the reputation score of a malicious target (or a destination) host name based on the reputation IP data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
solnGetTarget DomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget DomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationDo mainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetLowerT argetHostNam e	This variable returns the target host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetTarget ReputationHos tNameListEntr y	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttack erDomainLevel 2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttack erDomainLevel 1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttack erReputationH ostNameListEn try	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTarget ReputationDo mainLevel2List Entry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
Reputation Domain Enrichment	This field set contains fields with reputation domain information for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Reputation IP Enrichment	This field set contains fields with reputation IP information for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Request URL Enrichment	This field set contains fields with reputation information (based on the request URL) for event enrichment purposes.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Events with Requests to Malicious Hosts	This filter identifies events with requests to hosts found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/

Resource	Description	Type	URI
Events from Malicious Sources	This filter identifies events whose attackers are found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/
Events to Malicious Targets	This filter identifies events whose targets are found in the reputation database.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Events Enrichment with Reputation Data/

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

Resource	Description	Type	URI
Monitor Resources			
Internal Assets and Domains Found in Reputation Data	This dashboard provides information around internal assets or domain names reported in the reputation database.	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
All Internal IP Addresses Found	This query viewer shows all local IP addresses appeared in the reputation domain database.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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 the list should be investigated.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/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 hp.com or hp.co.uk.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
Internal IP Addresses Found in Reputation Data	This active list stores all local IP addresses that appear in the reputation IP database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
Internal Network Addresses for Reputation Monitoring	This active list stores all local public network addresses (only class A, B or C) to be monitored for existence in the reputation database. If your network does not use these classes (for example, it uses CIDR instead), you can use the smallest class that fully represents your network. For example, a network address of 192.168.1.1/26 can be represented by a class C network of 192.168.1.0, so you can put 192.168.0. in this list. Note that for each network address entry, a dot (.) character is required.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
All Internal IP Addresses Found	This query returns all local IPs appeared in the reputation domain database.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Assets Found in Reputation Data/

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Assets Found in Reputation Data/`
All Internal Domains Found	This query returns all local domains appeared in the reputation domain database.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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-6 Resources that Support the Internal Infected Assets Use Case

Resource	Description	Type	URI
Monitor Resources			
All Interactions with Malicious Entities Detected During the Last 2 Hours	This active channel shows all the occurrences of rules that fired to detect internal infections in this use case in the last two hours.	Active Channel	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`

Resource	Description	Type	URI
Open Case Status Distribution	This query viewer shows all open cases on internal infected assets, grouped by case status.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Summary of Contacted Malicious Entities	This query viewer shows the summary of malicious hosts contacted by infected internal hosts.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/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 domain names.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected 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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infection 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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infection Assets/
Library - Correlation Resources			

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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Infected Internal Assets: Outbound Communications to Malicious IPs	This rule captures all outbound traffic either from internal assets to reputation IP addresses with high scores and critical exploit types, or from public-facing assets to any reputation IP.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/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 span.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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 thus should be investigated carefully. By default, each asset in this list will be reported under a case opened. Once the case is closed, the asset will be automatically removed from this list.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`

Resource	Description	Type	URI
Protected	This is a site asset category.	Asset Category	`Site Asset Categories/Address Spaces`
Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/`
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
solnGetRequestURLDomainLevel3ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetTarget ReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`

Resource	Description	Type	URI
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetLowerTargetHostName	This variable returns the target host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationHostNameListEntry	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetDomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLReputationDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
Standard	null	Field Set	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Internal Infections	This field set provides the fields relevant to the correlation events generated by the detection rules in this use case.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Infected Assets: Outbound URL Requests to Malicious Domains	This filter identifies all outbound URL requests either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/

Resource	Description	Type	URI
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Infected Assets: Outbound Communicatio n 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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Outbound Communicatio n to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/

Resource	Description	Type	URI
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Infected Asset Count per Month	This query returns the count of internal infected assets per month over the last 1 year period.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Summary of Contacted Malicious Hosts	This query returns the summary of malicious hosts contacted by infected internal hosts.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Summary of Currently Infected Assets	This query returns the summary of internal infected machines detected through communications with reputation IPs or domains.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Internal Infected Asset Count per Week	This query returns the weekly count of internal infected assets over the last month.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Infection Types over Last Month	This query returns the weekly count of internal infected assets over the last month.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Status Distribution of Open Cases on Internal Infected Assets	This query returns all open cases on internal infected assets, grouped by case status.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Internal Infected Assets/
Daily Internal Infected Asset Snapshots	This trend stores snapshots of the internal infected asset list on a daily basis.	Trend	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/

RepSM Overview

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

Table D-7 Resources that Support the RepSM Overview Use Case

Resource	Description	Type	URI
Monitor Resources			
RepSM Overview	This dashboard provides an overview of traffic from reputation hosts in the last 24 hours (not real time).	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
Geographical View of Malicious Communications	This dashboard provides an overview of traffic to reputation hosts.	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Library - Correlation Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Access from Dangerous Sources: Successful Inbound Communications from Malicious Domain	This rule captures the first event of all successful inbound communications to internal, non public-facing assets from reputation domain names with zero day attack exploit types. It will open a case for each internal target.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/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 zero day attack exploit types. It will open a case for each internal target.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`

Resource	Description	Type	URI
Dangerous Browsing: Outbound Requests to Malicious Domains	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Dangerous Browsing: Outbound Communications to Malicious Domains	This rule captures all dangerous browsing activities from non public-facing assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Dangerous Browsing: Outbound Communications to Malicious IPs	This rule captures all dangerous browsing activities from non public-facing assets to reputation IP addresses with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Library Resources			
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant for zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, Miscellaneous.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with Zero-Day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/

Resource	Description	Type	URI
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/
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 7 days.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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 7 days.	Active List	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Public-Facing	This is a solutions asset category.	Asset Category	ArcSight Solutions/Reputation Security Monitor
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	ArcSight Solutions/Reputation Security Monitor
Recent Dangerous Browsing Destinations	This data monitor shows the last 20 dangerous browsing destinations from non public-facing internal assets.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
Attacks from Malicious Entities	This data monitor shows a geographical view of all (successful or failed) inbound communications from malicious hosts or IP addresses.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/

Resource	Description	Type	URI
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLReputationDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
solnGetAttackerReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerDomainExploitType	This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/

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	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetLowerTargetHostName	This variable returns the target host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerDomainLevel2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/

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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerDomainLevel1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationHostNameListEntry	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetTargetReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
Source Reputation Domain	This variable returns the reputation domain (or host name) related to a malicious attacker (or source) host name based on the reputation domain data.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
Events with Target Reputation Information	This field set contains fields with target reputation domain or IP address information.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
Events with Source Reputation Information	This field set contains fields with source reputation domain or IP address information.	Field Set	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Non Public-Facing Internal Targets	This filter identifies all events whose targets are categorized as non public-facing internal.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Reputation Outbound Communication	This filter identifies all communications to a malicious host or IP address.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
Internal Infected Asset Case Creation or Removal	This filter identifies events generated when the active list storing internal infection records is modified.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Zero Day Attack Reputation IP Exploit Types	This filter identifies events from malicious IP addresses having zero day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Inbound Communication from Malicious Domains	This filter identifies all inbound traffic from domain names in the reputation domain active list.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Dangerous Browsing Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
Zero Day Attack List Manipulation	This filter identifies events generated when the active list storing zero day attack records is modified.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/

Resource	Description	Type	URI
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Inbound Communicatio n from Malicious IP Addresses	This filter identifies all inbound traffic from IP addresses in the reputation IP active list for real time correlation.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Dangerous Browsing	This filter identifies all dangerous browsing activities.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Inbound Events	This filter identifies events coming from outside the network in your organization targeting the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Dangerous Browsing Target Reputation IP Exploit Types	This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/

Resource	Description	Type	URI
Outbound Communication to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Zero Day Attack Reputation Domain Exploit Types	This filter identifies events from malicious domain names or host names having zero-day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
Reputation Inbound Communication	This filter identifies all events from a malicious host or IP address.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Overview/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
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 7 days. It is based on a trend so it might not show most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Access from Dangerous Sources/
Access to Dangerous Destinations by Types During the Last 7 Days	This query returns the total count of access to dangerous destinations (domain, host name or IP address) during the last 7 days. It is based on a trend so it might not show most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Overview/
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 within the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
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 within the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Access to Dangerous Destinations/
Zero Day Attacks and Access from Dangerous Sources	This trend stores all firings of rules that detect zero day attacks or access from dangerous sources.	Trend	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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-8 Resources that Support the RepSM Package Health Status Use Case

Resource	Description	Type	URI
Monitor Resources			
Inbound Events	This active channel shows events the RepSM package considers as inbound.	Active Channel	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Outbound Events	This active channel shows events the RepSM package considers as outbound.	Active Channel	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
RepSM Rules Health	This dashboard provides an overview of rules in the RepSM package, including their status and logs.	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Events Analyzed by RepSM Use Cases	This dashboard provides an overview of the traffic monitored for reputation data.	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Library - Correlation Resources			

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Dangerous Browsing: Outbound Requests to Malicious Domains	This rule captures all dangerous browsing activities with URL requests from non public-facing internal assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Internal Domain Found in Reputation Data	This rule detects when an internal domain appears in the reputation domain database.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Dangerous Browsing: Outbound Communications to Malicious Domains	This rule captures all dangerous browsing activities from non public-facing assets to reputation domain names with high scores and non-critical exploit types.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Internal IP Address Found in Reputation Data	This rule detects when an internal address appears in the reputation IP database.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Assets Found in Reputation Data/

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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Access from Dangerous Sources: Successful Inbound Communications from Malicious Domain	This rule captures the first event of all successful inbound communications to internal, non public-facing assets from reputation domain names with zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
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 zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Dangerous Browsing: Outbound Communications to Malicious IPs	This rule captures all dangerous browsing activities from non public-facing assets to reputation IP addresses with high scores and non-critical exploit types.	Rule	`ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/`
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant for zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, Miscellaneous.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`
Critical Exploit Types	This active list contains all exploit types considered as critical for monitoring purposes.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with Zero-Day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Dangerous Browsing Exploit Types	This active list contains all exploit types considered as dangerous browsing. By default, it contains Malware and Phishing.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`

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 thus should be investigated carefully. By default, each asset in this list will be reported under a case opened. Once the case is closed, the asset will be automatically removed from this list.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/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 span.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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 7 days.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/`
Malicious Host Names in Dangerous Sources Access and Zero Day Attacks	This active list stores all malicious host names involved in interactions with dangerous sources and zero day attacks. It is used internally to show all base events, and has a time-to-live of 7 days.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Protected	This is a site asset category.	Asset Category	`Site Asset Categories/Address Spaces`

Resource	Description	Type	URI
Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	`ArcSight Solutions/Reputation Security Monitor`
Top Firing Rules	This data monitor shows the reputation-traffic monitoring rule with most firings.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Rule 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 will be changed to Successful. If an error occurs and the trend query fails, the trend state will be set to Failed.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Trend 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 are events monitored by the Zero Day Attacks use case.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Event Statistics/`
RepSM Trend Query Duration	This Last N Events Data Monitor shows the duration of the last 20 successful Trend queries. This Data Monitor is used in the Trends Status Dashboard.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Trend Health/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Event Statistics/`
Messages from Model Import Connector for RepSM	This data monitor shows important messages from the model import connector for RepSM. These messages ensure the connector is working properly or help troubleshoot any issues.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/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 are events monitored by the Access from Dangerous Sources use case.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Event Statistics/`

Resource	Description	Type	URI
RepSM Rule States	This Last State data monitor shows the states (enabled, disabled or deleted) of the RepSM rules.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Rule Health/
Last 10 RepSM Trend Query Failures	This Last N Events data monitor shows the last 10 trend query failures.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Trend 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	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Event Statistics/
Last 10 RepSM Trend Queries Returning No Results	This Last N Events data monitor shows the last 10 trend queries returning no results.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Trend Health/
Recently Triggered Rules	This data monitor shows the ten recent RepSM rules that fired.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Rule Health/
RepSM Rule Error Logs	This data monitor shows the internal audit events related to RepSM rules. These events are generated when the rules are enabled/disabled or removed.	Data Monitor	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/Rule Health/
solnGetTarget DomainLevel4	This variable returns the 4 right most subdomains of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTarget ReputationIPListEntry	This variable returns the target address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetRequestURLDomainLevel1	This variable returns the right most subdomain of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/

Resource	Description	Type	URI
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetBaseRequestURLDomainEntry	This variable returns the entry of a base request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2	This variable returns the two rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainExploitType	This variable returns the exploit type of the request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetTargetDomainLevel1	This variable returns the right most (top) subdomain of a target's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLReputationDomainEntry	This variable returns the entry of a request URL in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel3	This variable returns the three rightmost subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerDomainExploitType	This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel3ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
solnGetRequestURLDomainLevel1ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 1.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
solnGetTargetDomainLevel2	This variable returns the two rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTargetDomainLevel3	This variable returns the three rightmost subdomains of a target's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTargetReputationDomainEntry	This variable returns the entry of a target in the reputation domain list used for real time correlation.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/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	`ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/`
solnGetLowerTargetHostName	This variable returns the target host name in lower case.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetTargetReputationHostNameListEntry	This variable returns the entry of a target host name in the reputation domain list used for real time correlation.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/`
solnGetAttackerDomainLevel2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`
solnGetAttackerDomainLevel1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	Global Variable	`ArcSight Solutions/Reputation Security Monitor 1.0/Support/`

Resource	Description	Type	URI
solnGetAttackerReputationHostNameListEntry	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetTargetReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel2ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetTargetReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the target domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Non Public-Facing Internal Targets	This filter identifies all events whose targets are categorized as non public-facing internal.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/

Resource	Description	Type	URI
Events Monitored by Zero Day Attack Use Case	This filter identifies all events monitored by Zero Day Attacks use case. These are events reflecting inbound communications to assets categorized as internal, non public-facing.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Dangerous Browsing Activities - Rule Firings	This filter identifies all firings of rules that detect dangerous browsing activities.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Dangerous Browsing/
Infected Assets: Outbound Communicatio n 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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Infected Assets: Outbound URL Requests to Malicious Domains	This filter identifies all outbound URL requests either from internal assets to reputation domain names with high scores and critical exploit types, or from public-facing assets to any reputation domain.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
Events Monitored by Access from Dangerous Sources Use Case	This filter identifies all events monitored by Access from Dangerous Sources use case. These are events reflecting inbound communications to all assets.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
RepSM Trend Query Failure	This Filter is looking for failed RepSM trend query runs events.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Dangerous Destinations and Dangerous Browsing: Outbound Communicatio n 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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Outbound Events	This filter identifies events coming from inside the network in your organization targeting the public network.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/

Resource	Description	Type	URI
Zero Day Attack Reputation IP Exploit Types	This filter identifies events from malicious IP addresses having zero day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
Critical Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with critical exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
Inbound Communication from Malicious Domains	This filter identifies all inbound traffic from domain names in the reputation domain active list.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
Public-Facing Attackers	This filter identifies all events whose attackers are categorized as public-facing assets.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Access from Dangerous Sources - Rule Firings	This filter identifies all correlation events generated by rules that detect access from dangerous sources.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
Dangerous Browsing Request Domain Exploit Types	This filter identifies requested URLs to reputation domain or host name with dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
Events Monitored by Internal Infected Assets Use Case	This filter identifies all events monitored by Internal Infected Assets use case. These are events containing request URLs, or reflecting outbound communications.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/

Resource	Description	Type	URI
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
RepSM Rule Firing Events	This filter identifies all RepSM rule firings.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Critical Target Reputation Domain Exploit Types	This filter identifies critical target reputation domain or host name exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
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 are events containing request URLs, or reflecting outbound communications from assets not categorized as Public-Facing.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Critical Target Reputation IP Exploit Types	This filter identifies critical target reputation IP exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/Support/
RepSM Trend Query Duration	This Filter is looking for successful RepSM trend query runs events.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Interactions with Dangerous Destinations - Rule Firings	This filter identifies all firings of rules that detect interactions with dangerous destinations (i.e. non-browsing exploit types).	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/

Resource	Description	Type	URI
RepSM Trend Query Returning No Results	This Filter is looking for successful RepSM trend query runs events where the number of rows inserted in the trend is 0.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Target Host Name Present	This filter checks if the Target Host Name field is populated.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Inbound Events	This filter identifies events coming from outside the network in your organization targeting the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Zero Day Attacks - Rule Firings	This filter identifies all correlation events generated by rules that detect zero day attacks.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
RepSM Rules Engine Events	This filter identifies all internal audit events related to RepSM rules.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Dangerous Browsing Target Reputation IP Exploit Types	This filter identifies events to target reputation IP addresses considered as of dangerous browsing exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Internal Infected Assets/
RepSM Trend Runs Status	This Filter is looking for trend query runs events.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
Outbound Communication to Reputation IP Addresses	This filter identifies all outbound traffic to reputation IP addresses.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Zero Day Attack Reputation Domain Exploit Types	This filter identifies events from malicious domain names or host names having zero-day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/

Resource	Description	Type	URI
Events from Model Import Connector for RepSM	This filter identifies important events generated by the RepSM Model Import Connector.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/RepSM Package Health Status/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Access to Dangerous Destinations/Support/

Reputation Data Analysis

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

Table D-9 Resources that Support the Reputation Data Analysis Use Case

Resource	Description	Type	URI
Monitor Resources			
Reputation Domain Database Overview	This dashboard shows an overview of the reputation domain database (stored in an active list) in the system.	Dashboard	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation Domain Exploit Type Distribution	This query viewer shows the reputation domain count per exploit type.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation IP Exploit Type Distribution	This query viewer shows the reputation address count per exploit type.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/

Resource	Description	Type	URI
Reputation IP Entries	This query viewer shows the top 1,000,000 IP entries in the reputation IP active list.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation IP Entry Count	This query viewer shows the current number of reputation addresses.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation Domain Type Distribution	This query viewer shows the distribution of entries in the reputation domain database.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation Domain Score Histogram	This query viewer shows the histogram of the reputation domain score.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation Domain Entries	This query viewer shows the top 1,000,000 domain entries in the reputation domain active list.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/
Reputation IP Score Histogram	This query viewer shows the histogram of the reputation IP score.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/

Resource	Description	Type	URI
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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 within the last 8 hours.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/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 within the last 8 hours.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/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 is operating properly and periodically updates the list.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/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 is operating properly and periodically updates the list.	Data Monitor	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/`
Reputation IP Changes	This filter identifies events when a change is made to the reputation IP address active list.	Filter	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Database Analysis/`
Reputation Domain Changes	This filter identifies events when a change is made to the reputation domain active list.	Filter	`ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Database Analysis/`
Reputation IP Changes - Trend Base	This query returns the count of reputation addresses, grouped by the exploit type.	Query	`ArcSight Solutions/Reputation Security Monitoring 1.0/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 one week period.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 one week.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain Changes During the Last 1 Week	This query returns the count of reputation domain entries during the last one week.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP by Exploit Type	This query returns the count of reputation addresses per exploit type.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain by Exploit Type	This query returns the reputation domain count per exploit type.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain Entry Count by Type	This query returns the current count of reputation domains and host names.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP Changes During the Last 1 Week	This query returns the count of reputation addresses during the last one week.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP Score Histogram	This query builds the histogram of the reputation IP score.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain Score Histogram	This query builds the histogram of the reputation domain score.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 one year.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/

Resource	Description	Type	URI
Reputation Domain Changes During the Last 1 Year	This query returns the monthly average count of reputation domain entries during the last one year.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain Changes by Type During the Last 1 Week	This query returns the count of reputation domain exploit types during the last one week period.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 one week.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP Entries	This query returns the top 1000000 IP entries in the reputation IP active list.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 one year.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation Domain Entries	This query returns the top 1000000 domain entries in the reputation domain active list.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 one year period.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP Entry Count	This query returns the current number of reputation addresses.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Reputation Database Analysis/
Reputation IP changes	This trend stores the daily count of reputation IP entries, grouped by the exploit type.	Trend	ArcSight Solutions/Reputation Security Monitor 1.0/Reputation Data Analysis/

Resource	Description	Type	URI
Reputation Domain Changes	This trend stores the daily count of reputation domain names, grouped by the exploit type.	Trend	ArcSight Solutions/Reputation Security Monitor 1.0/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-10 Resources that Support the Zero Day Attacks Use Case

Resource	Description	Type	URI
Monitor Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Zero Day Attack Cases	This query viewer shows all open cases on zero day attacks, grouped by case status.	Query Viewer	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Library - Correlation Resources			
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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Access from Dangerous Sources: Successful Inbound Communications from Malicious Domain	This rule captures the first event of all successful inbound communications to internal, non public-facing assets from reputation domain names with zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/
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 zero day attack exploit types. It will open a case for each internal target.	Rule	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`
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	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Library Resources			
Malicious IP Addresses	This active list stores up to 1 million reputation IP addresses from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
Zero Day Attack Exploit Types	This active list contains all exploit types considered as relevant for zero day attacks. By default, it contains Web Application Attacker, P2P, Botnet, Worm, Misuse and Abuse, Miscellaneous.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`
Zero Day Attacks and Access from Dangerous Sources	This list contains all successful inbound communications from a malicious host with Zero-Day attack exploit type. The lists of such exploit types are defined by the Zero Day Attack Exploit Types active list.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Malicious Domains	This active list stores up to 1 million reputation domain names from the RepDV database.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/`
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 7 days.	Active List	`ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/`
Protected	This is a site asset category.	Asset Category	`Site Asset Categories/Address Spaces`
Internal Non Public-Facing	This is a solutions asset category.	Asset Category	`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	`ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/`

Resource	Description	Type	URI
solnGetAttackerReputationDomainLevel1ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 1.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerDomainExploitType	This variable returns the exploit type of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel3	This variable returns the three rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGenericHighScoreThreshold	This global variable defines the generic threshold for high reputation scores.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetRequestURLDomainLevel4ListEntry	This variable returns the entry in the reputation domain database corresponding to the request URL domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetLowerAttackerHostName	This variable returns the attacker host name in lower case.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainEntry	This variable returns the entry of an attacker in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
solnGetAttackerDomainLevel4	This variable returns the 4 right most subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/

Resource	Description	Type	URI
solnGetAttackerDomainLevel2	This variable returns the two rightmost subdomains of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerDomainLevel1	This variable returns the right most subdomain of an attacker's host name that follows the dotted format.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation Data/
solnGetAttackerReputationHostNameListEntry	This variable returns the entry of an attacker host name in the reputation domain list used for real time correlation.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
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	ArcSight Solutions/Reputation Security Monitor 1.0/Event Enrichment with Reputation 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	ArcSight Solutions/Reputation Security Monitor 1.0/Configuration/
solnGetAttackerReputationDomainLevel2ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 2.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerReputationDomainLevel4ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 4.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetAttackerReputationDomainLevel3ListEntry	This variable returns the entry in the reputation domain list corresponding to the attacker domain level 3.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/
solnGetRequestURLDomain	This variable returns the domain substring of a request URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/
solnGetRequestURLDomainLevel4	This variable returns the 4 right most subdomains of the requested URL.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Support/

Resource	Description	Type	URI
solnGetAttackerReputationIPListEntry	This variable returns the attacker address entry in the reputation IP database.	Global Variable	ArcSight Solutions/Reputation Security Monitor 1.0/Main Final Variables/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Zero Day Attack Reputation IP Exploit Types	This filter identifies events from malicious IP addresses having zero day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
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	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Non Public-Facing Internal Targets	This filter identifies all events whose targets are categorized as non public-facing internal.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Inbound Communication from Malicious Domains	This filter identifies all inbound traffic from domain names in the reputation domain active list.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/Malicious Communications/
Internal Attackers	This filter identifies events coming from systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Inbound Events	This filter identifies events coming from outside the network in your organization targeting the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/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	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/
Zero Day Attacks - Rule Firings	This filter identifies all correlation events generated by rules that detect zero day attacks.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/

Resource	Description	Type	URI
Internal Targets	This filter identifies events targeting systems inside the network in your organization.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/General/
Zero Day Attack Reputation Domain Exploit Types	This filter identifies events from malicious domain names or host names having zero-day attack exploit types.	Filter	ArcSight Solutions/Reputation Security Monitor 1.0/Zero Day Attacks/Support/
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	ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 1 year. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
Status Distribution of Open Case on Zero Day Attacks	This query returns all open cases on zero day attacks, grouped by case status.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/

Resource	Description	Type	URI
Top Assets Most Attacked During the Last 7 Days	This query returns the internal assets received most zero day attacks during the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
Zero Day Attacks in the Last 24 Hours	This query returns all zero day attacks in the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
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 1 year. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 within the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/

Resource	Description	Type	URI
Top Attacked Assets During the Last 24 Hours	This query returns the internal assets being attacked the most during the last 24 hours.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
Zero Day Attack Details During the Last 7 Days	This query returns the details of zero day attacks within the last 7 days. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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 7 days. It is based on a trend so it might not show most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/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	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
Zero Day Attacks per Reputation Type During the Last One Year	This query returns the number of zero day attacks per reputation (exploit) type within the last 1 year. This query is based on a trend so it might not show the most recent data.	Query	ArcSight Solutions/Reputation Security Monitoring 1.0/Zero Day Attacks/
Zero Day Attacks and Access from Dangerous Sources	This trend stores all firings of rules that detect zero day attacks or access from dangerous sources.	Trend	ArcSight Solutions/Reputation Security Monitor 1.0/Access from Dangerous Sources/

Index

A

C

D

E

F

G

I

L

M

N

O

P

Q

R

S

T

U

W

Z