



# HP ArcSight ESM

Software Version: 6.8c

## Intrusion Monitoring Standard Content Guide

November 17, 2014

## Legal Notices

### Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

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

<http://www.hpenterprisesecurity.com/copyright>

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support Page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hp.com">https://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.hp.com">https://protect724.hp.com</a>

# Contents

Chapter 1: Intrusion Monitoring Overview .....	5
What is Standard Content? .....	5
Standard Content Packages .....	7
Intrusion Monitoring Content .....	8
Chapter 2: Installation and Configuration .....	9
Installing the Intrusion Monitoring Package .....	9
Modeling the Network .....	10
Categorizing Assets .....	11
Configuring Active Lists .....	11
Configuring Rules .....	12
Configuring the Network Management Filter .....	12
Configuring Notification Destinations .....	13
Configuring Notifications and Cases .....	13
Scheduling Reports .....	14
Restricting Access to Vulnerability View Reports .....	14
Configuring Trends .....	14
Chapter 3: Intrusion Monitoring Content .....	16
Alerts from IDS-IPS .....	18
Alerts from IDS-IPS Resources .....	18
Anti-Virus Activity and Status .....	21
Anti-Virus Activity and Status Resources .....	21
Attack Rates .....	29
Configuring the Attack Rates Resource Group .....	29
Attack Rates Resources .....	29
Attackers .....	41
Attackers Resources .....	41
Business Impact Analysis .....	67
Configuring the Business Impact Analysis Resource Group .....	67
Business Impact Analysis Resources .....	67

DoS .....	72
Configuring the DoS Resource Group .....	72
DoS Resources .....	72
Environment State .....	81
Environment State Resources .....	81
Login Tracking .....	92
Configuring the Login Tracking Resource Group .....	92
Login Tracking Resources .....	92
Reconnaissance .....	121
Configuring the Reconnaissance Resource Group .....	121
Reconnaissance Resources .....	122
Regulated Systems .....	149
Configuring the Regulated Systems Resource Group .....	149
Regulated Systems Resources .....	149
Resource Access .....	152
Configuring the Resource Access Resource Group .....	152
Resource Access Resources .....	153
Revenue Generating Systems .....	165
Revenue Generating Systems Resources .....	165
SANS Top 5 Reports .....	169
SANS Top 5 Reports Resources .....	169
SANS Top 20 .....	173
Configuring the SANS Top 20 Resource Group .....	173
SANS Top 20 Resources .....	173
Security Overview .....	202
Configuring the Security Overview Resource Group .....	202
Security Overview Resources .....	202
Targets .....	217
Targets Resources .....	217
Vulnerability View .....	238
Vulnerability View Resources .....	238
Worm Outbreak .....	246
Worm Outbreak Resources .....	246
Send Documentation Feedback .....	252

# Chapter 1: Intrusion Monitoring Overview

This chapter discusses the following topics.

What is Standard Content? .....	5
Standard Content Packages .....	7
Intrusion Monitoring Content .....	8

## What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

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

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
  - ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
  - ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.

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

- ArcSight Content Management is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information

includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- ArcSight ESM HA Monitoring is an optional package that lets you monitor systems that use the ESM High Availability Module. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.
- ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the *ArcSight Command Center User's Guide*.

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

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality. The ArcSight Networks package contains the zones that were in the ArcSight Core package in previous releases, in addition to local and global network resources.
- **ArcSight Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
  - Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
  - Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
  - Global Variables content is a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and

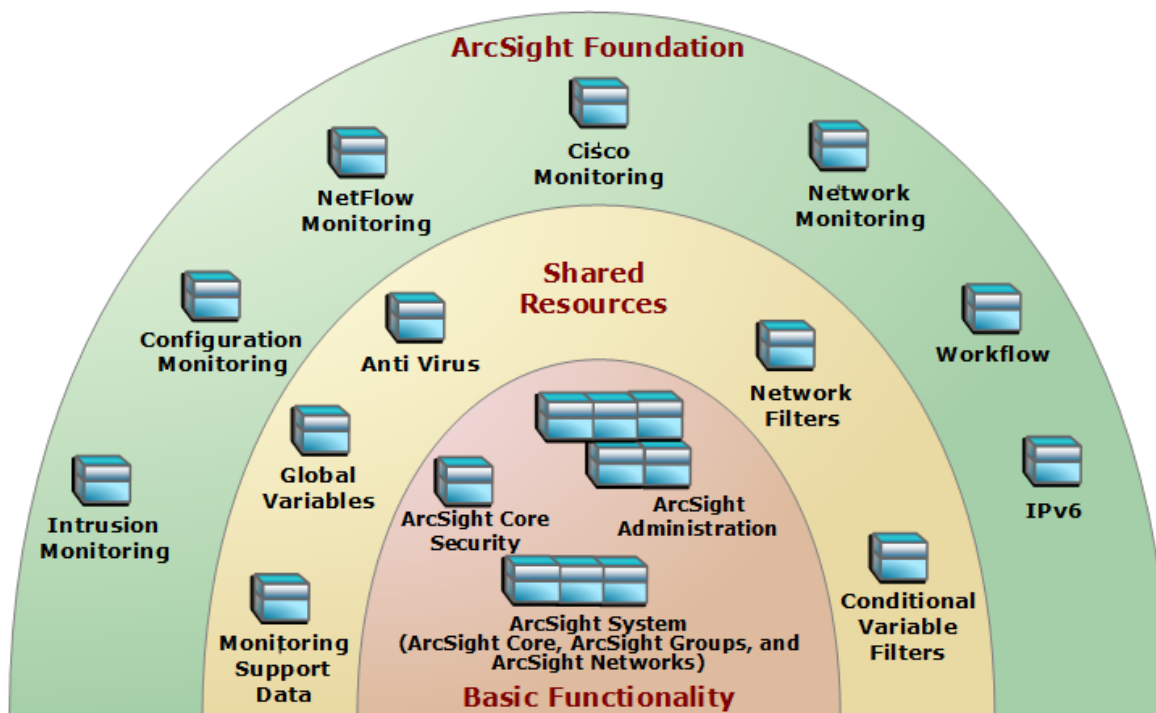
commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.

- Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
- Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

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

## Standard Content Packages

Standard content comes in packages (.arb files) that are either installed automatically or presented as install-time options. The following graphic outlines the packages.



The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you install, you will see the ArcSight Core Security, ArcSight Administration, and ArcSight System resources and some or all of the other package content.

**Caution:** When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the *ArcSight Console User's Guide*.

## Intrusion Monitoring Content

The Intrusion Monitoring content is a coordinated set of resources that identify hostile activity and take appropriate action. The content provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting.

The Intrusion Monitoring content targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and more. This content also addresses several of the SANS top 20 list of vulnerable areas.

This guide describes the Intrusion Monitoring content. For information about ArcSight Core Security, ArcSight Administration, or ArcSight System content, refer to the *ArcSight Core Security*, *ArcSight Administration*, and *ArcSight System Standard Content Guide*. For information about an optional ArcSight Foundation, refer to the Standard Content Guide for that Foundation. ESM documentation is available on [Protect 724](https://protect724.hp.com) (<https://protect724.hp.com>).



## Chapter 2: Installation and Configuration

This chapter discusses the following topics:

Installing the Intrusion Monitoring Package .....	9
Modeling the Network .....	10
Categorizing Assets .....	11
Configuring Active Lists .....	11
Configuring Rules .....	12
Configuring the Network Management Filter .....	12
Configuring Notification Destinations .....	13
Configuring Notifications and Cases .....	13
Scheduling Reports .....	14
Restricting Access to Vulnerability View Reports .....	14
Configuring Trends .....	14

### Installing the Intrusion Monitoring Package

The Intrusion Monitoring Foundation package is one of the standard content packages presented as install-time options. If you selected all the standard content packages to be *installed* at installation time, the packages and their resources are installed in the ArcSight Database and available in the Navigator panel resource tree. The package icons in the Navigator panel package view appear blue.

If you opted to exclude a Foundation package during ArcSight Manager installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears grey.

#### To install a package that is imported, but not installed:

1. On the Navigator panel Packages tab, navigate to the package you want to install.
2. Right-click the package and select **Install Package**.
3. In the Install Package dialog, click **OK**.
4. When the installation is complete, review the summary report and click **OK**.

The package resources are fully installed to the ArcSight Database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

**To uninstall a package that is installed:**

1. On the Navigator Panel Packages tab, navigate to the package you want to uninstall.
2. Right-click the package and select **Uninstall Package**.
3. In the Uninstall Package dialog, click **OK**.
4. 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 uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight Database and the Navigator panel resource tree, but remains available in the Navigator panel Packages tab, and can be re-installed at another time.

If you do not want the package to be available in any form, you can *delete* the package.

**To delete a package and remove it from the ArcSight Console and the ArcSight Database:**

1. On the Navigator Panel Packages tab, navigate to the package you want to delete.
2. Right-click the package and select **Delete Package**.
3. When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

## Modeling the Network

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

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

## Categorizing Assets

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

Asset Category	Description
/Site Asset Categories/ Address Spaces/Protected	<p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as <i>Protected</i>.</p> <p><b>Note:</b> Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p>
/System Asset Categories/ Criticality/High	<p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.</p>
/System Asset Categories/ Criticality/Very High	Same as /System Asset Categories/ Criticality/High

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

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

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

## Configuring Active Lists

The standard content includes active lists. Certain active lists are populated automatically during run-time by rules. You do not have to add entries to these active lists manually before you use them. Other active lists are designed to be populated *manually* with data specific to your environment. After the lists

are populated with values, they are cross-referenced by active channels, filters, rules, reports, and data monitors to give ESM more information about the assets in your environment.

Intrusion Monitoring content uses the following active lists that you need to populate manually:

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

You can add entries manually to active lists using the following methods. Both methods are described in the *ArcSight Console User's Guide*.

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

## Configuring Rules

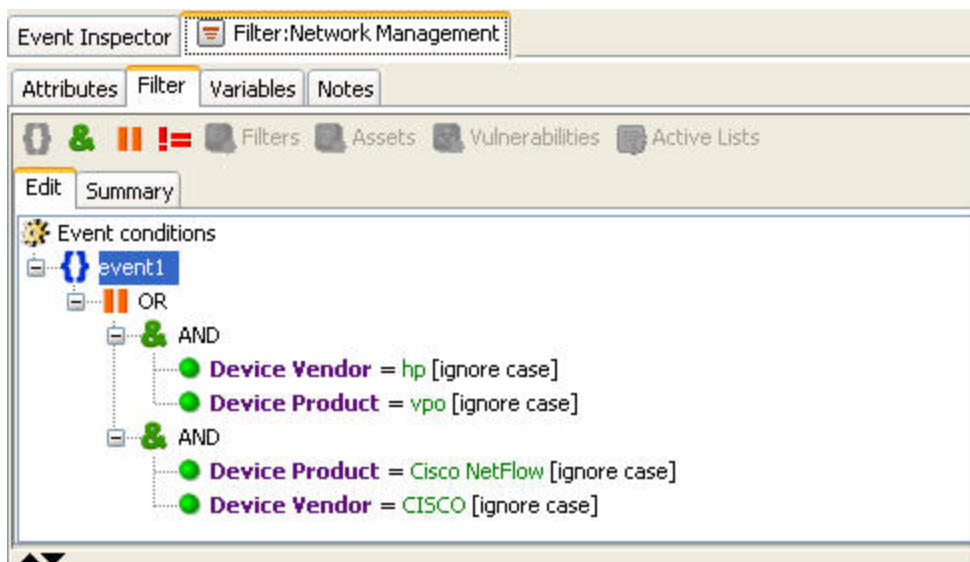
Rules trigger only if they are deployed in the `Real-Time Rules` group and are enabled. All Intrusion Monitoring rules are deployed by default in the `Real-Time Rules` group and are enabled.

**To disable a rule:**

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

## Configuring the Network Management Filter

The Network Management filter (`/All Filters/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Network Management`) identifies events from two network management devices: HP VPO and Cisco NetFlow. If you use a network management device other than these, modify this filter with the Device Vendor and Device Product name of the device you use. The example below shows the default conditions in the Network Management filter.



You can add to these conditions, or remove the existing ones and create new ones.

## Configuring Notification Destinations

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

Refer to the *ArcSight Console User's Guide* for information on how to configure notification destinations.

## Configuring Notifications and Cases

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

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

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

## Scheduling Reports

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

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

## Restricting Access to Vulnerability View Reports

The Vulnerability View detail reports display a list of vulnerabilities generated by scanner report events, and are therefore considered sensitive material. By default, the reports are configured with read access for Administrators, Default User Groups, and Analyzer Administrators. Administrators and Analyzer Administrators also have write access to this group.

To eliminate these events from view, you need to create a special filter and apply the filter to the appropriate users groups. Before deciding whether to restrict access to the Vulnerability View reports, be aware of the following:

- Because access is inherited, the parent group must have the same or more liberal permissions than the vulnerability reports.
- If you need to move the reports to a group with tighter permissions, also move the trends and queries that support them, in both the Detail and Operational Summaries sections.
- To get a complete view of the resources attached to these reports, run a resource graph on the individual filters or the parent group (right-click the resource or group and select **Graph View**).

## Configuring Trends

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

Intrusion Monitoring content includes several trends, some of which are enabled by default. These enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m. when network traffic is usually less busy than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the ArcSight Console.

To disable or enable a trend, go to the **Trend** tab from the **Reports** drop-down list in the Navigator panel, right-click the trend, then select **Disable Trend** or **Enable Trend**.

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

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

## Chapter 3: Intrusion Monitoring Content



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

Resource Group	Purpose
"Alerts from IDS-IPS" on page 18	"The Alerts from IDS-IPS resources provide information about alerts from Intrusion Detection Systems and Intrusion Prevention Systems. "
"Anti-Virus Activity and Status" on page 21	"The Anti-Virus Activity and Status resources provide information about virus activity by using two moving average data monitors that track increases in virus activity either by zone or by host, and the Virus Activity event graph."
"Attack Rates" on page 29	"The Attack Rates resources provide information about changes in attack activity by either service or target zone. The reports are driven by moving average data monitors. The dashboards display the appropriate data monitors for a view of the areas (services and target zones), to assist in determining whether the network is being attacked in a general sense, or if the attacks focus on specific network areas."
"Attackers" on page 41	"The Attackers resources provide statistics about attackers (such as reporting device, target host, target port, and ArcSight priority), views of attackers (by attacker port and, when available, by protocol), and statistics about attackers by using top and bottom 10 lists. The bottom 10 lists can be useful for tracking the attackers who are trying to avoid detection by the low-and-slow method (low volume over a long period of time)."
"Business Impact Analysis" on page 67	"The Business Impact Analysis resources provide information about which business areas are the victims of the most attack activity."
"DoS" on page 72	"The DoS (Denial of Service) resources use moving average data monitors and categorized events with the technique set to /DoS to help determine when a DoS is taking place. The data monitors highlight high-volume activity that might result in a DoS. The categorized events (mostly from an IDS) can show DoS events that do not require exceeding bandwidth or processing limitations."
"Environment State" on page 81	"The Environment State resources provide information about activity that reflects the state of the overall network, and provide details about applications, operating systems and services. "
"Login Tracking" on page 92	"The Login Tracking resources provide information about user logins."



Resource Group	Purpose
"Reconnaissance" on page 121	"The Reconnaissance resources expand on the ArcSight Core reconnaissance rules, and provide insight into the different types of reconnaissance directed at the network or parts of the network. This content breaks down reconnaissance activity by type. Dashboards show what parts of the network are being scanned and how. "
"Regulated Systems" on page 149	"The Regulated Systems resources focus on events related to assets that have been categorized as one of the compliance requirement asset categories, such as HIPAA, Sarbanes-Oxley, and FIPS-199."
"Resource Access" on page 152	"The Resource Access resources focus on access events, broken down by resource types, such as (database, email, files, and so on) and track this access by user. The brute force resource activity is included here. There are session lists that track the duration of an access session by user, and the duration of access sessions that took place after a brute force login attack."
"Revenue Generating Systems" on page 165	"The Revenue Generating Systems resources provide reports that focus on attacked or compromised systems that have been categorized in the Revenue Generation category under Business Impact Analysis/Business Roles."
"SANS Top 5 Reports" on page 169	"The SANS Top 5 Reports resources provide information that helps address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports."
"SANS Top 20" on page 173	"The SANS Top 20 resources provide the context for a series of email and operating system rules that look for specific events that relate to vulnerabilities. The SANS Top 20 reports show assets where these vulnerabilities have been compromised."
"Security Overview" on page 202	"The Security Overview resources provide information of interest to executive level personnel."
"Targets" on page 217	"The Targets resources provide security information focused on target information."
"Vulnerability View" on page 238	"The Vulnerability View resources provide information about assets and their vulnerabilities, with an active channel that focuses on vulnerability scanner reports. These resources present two major reports that are a variation on the list of assets and the list of vulnerabilities."
"Worm Outbreak" on page 246	"The Worm Outbreak resources provide information about worm activity and the affect a worm has had on the network."

## Alerts from IDS-IPS

The Alerts from IDS-IPS resources provide information about alerts from Intrusion Detection Systems and Intrusion Prevention Systems.

The following device types can supply events that apply to the resources in the Alerts from IDS-IPS resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Alerts from IDS-IPS Resources

The following table lists all the resources in the Alerts from IDS-IPS group.

### Resources that Support the Alerts from IDS-IPS Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Top Alerts from IDS and IPS	This report shows the top alerts coming from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Alert Counts per Hour	This report shows the total count of IDS and IPS alerts per hour during the past 24 hours (by default).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Device	This report shows the count of IDS and IPS alerts by device. A chart shows the top ten device addresses with the highest counts. A table shows the list of all the devices, grouped by device vendor and product, then sorted by count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/

**Resources that Support the Alerts from IDS-IPS Group, continued**

Resource	Description	Type	URI
Alert Counts by Port	This report shows the count of IDS and IPS alerts by destination port. A chart shows the top ten ports with the highest counts. A table shows the list of all the counts sorted in descending order.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Severity	This report shows the total count of IDS and IPS alerts by agent severity. A chart shows the count of alerts by severity. A table shows the count of alerts by severity, device vendor, and device product.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Type	This report shows the count of IDS and IPS alerts by type (category technique). A chart shows the top ten alert counts. A table shows the list of all the counts sorted in descending order.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
<b>Library Resources</b>			
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Base events.	Filter	/All Filters/ArcSight Core Security/IDS-IPS Monitoring
All Events	This filter matches all events.	Filter	ArcSight System/Core
Top 10 Alerts	This report shows the top alerts that originate from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Severity (Chart)	This query returns the count of IDS and IPS alerts by severity (agent severity).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Port	This query returns the count of IDS and IPS alerts by destination port.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Type	This query selects the count of IDS and IPS alerts by type (category technique).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/

**Resources that Support the Alerts from IDS-IPS Group, continued**

Resource	Description	Type	URI
Top IDS and IPS Alerts	This query returns IDS and IPS alert events, selecting the device event class ID, event name, device vendor, device product, and a count on the end time of the event.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top Alerts from IDS/
Alert Counts by Severity	This query returns the count of IDS and IPS alerts by severity (agent severity), device vendor, and device product.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts by Device	This query returns the count of IDS and IPS alerts by device vendor, product, zone, address, and hostname.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Alert Counts per Hour	This query returns the count of IDS and IPS alerts per hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table

## Anti-Virus Activity and Status

The Anti-Virus Activity and Status resources provide information about virus activity by using two moving average data monitors that track increases in virus activity either by zone or by host, and the Virus Activity event graph.

The following device types can supply events that apply to the resources in the Anti-Virus Activity and Status resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Vulnerability scanners

## Anti-Virus Activity and Status Resources

The following table lists all the resources in the Anti-Virus Activity and Status group.

### Resources that Support the Anti-Virus Activity and Status Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Virus Activity Statistics	This dashboard displays data monitors showing virus activity by zone and by host.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/
Anti-Virus Overview	This dashboard shows an overview of the top infections, the top infected systems, and the most recent and top anti-virus error events.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Virus Activity Overview	This dashboard displays data monitors showing virus activity and is based on the Virus Activity Statistics dashboard. The Virus Activity data monitor shows a graph view of the viruses, their relationships to the infected systems, and the relationships of the infected systems to the network zones. The Virus Activity by Zone and Virus Activity by Host data monitors are moving average graphs grouping by virus name, target zone resource, and address and customer resource.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/
Errors Detected in Anti-Virus Deployment	This report displays the hosts reporting the most anti-virus errors for the previous day and includes the anti-virus product, host details, error information, and the number of errors.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus
Top Infected Systems	This report displays summaries of the systems reporting the most infections during the previous day.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus
Failed Anti-Virus Updates	This report displays a table with the anti-virus vendor and product name as well as the hostname, zone, and IP address of the host on which the update failed. The time (EndTime) at which the update failed is also displayed. This report runs against events that occurred yesterday.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus
Virus Activity by Time	This report displays malware activity by hour for the previous day by hour and priority.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Update Summary	This report displays a summary of the results of anti-virus update activity by zones since yesterday.	Report	ArcSight Foundation/Configuration Monitoring/Details/Configuration Changes/Device/Anti-Virus
<b>Library Resources</b>			
Top 10 Infected Systems	This data monitor shows the top ten systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Anti-Virus Overview/
Top 10 Anti-Virus Errors	This data monitor shows the top ten errors experienced by Anti-Virus systems with events matching the Anti-Virus Errors filter.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Anti-Virus Overview/
Virus Activity	This data monitor shows the virus activity on the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Virus Activity Overview/
Top 10 Infections	This data monitor shows the top ten infections with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Anti-Virus Overview/
Virus Activity by Host	This data monitor shows the most active hosts with virus activity on the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Virus Activity Overview/
Virus Activity by Zone	This data monitor shows the most active zones with virus activity on the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Virus Activity Overview/

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Last 10 Anti-Virus Errors	This data monitor tracks the last anti-virus error events, displaying the time of occurrence, the priority, the vendor information, and the device information.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Anti-Virus Overview/
Virus Information	This field set displays useful fields for evaluating anti-virus events.	Field Set	ArcSight Foundation/Common/Anti-Virus
Anti-Virus Events	This filter identifies events in which the category device group is /IDS/Host/Antivirus.	Filter	ArcSight Foundation/Common/Anti-Virus
Virus Activity	This filter detects virus activity reported by either an IDS or a anti-virus application. The filter classifies virus events in two ways: The Category Object starts With /Vector/Virus or /Host/Infection/Virus, or the Category Behavior is /Found/Vulnerable, starts with /Modify/Content or /Modify/Attribute, and has a Category Device Group of /IDS/Host/Antivirus and the Device Custom String1 is set to some value.	Filter	ArcSight Foundation/Common/Anti-Virus
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
AV - Found Infected	This filter identifies all events where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable.	Filter	ArcSight Foundation/Common/Anti-Virus



**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Anti-Virus Errors	This filter identifies events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational.	Filter	ArcSight Foundation/Common/Anti-Virus
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
Update Events	This filter identifies events related to anti-virus product data file updates.	Filter	ArcSight Foundation/Common/Anti-Virus
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host
All Events	This filter matches all events.	Filter	ArcSight System/Core
AV - Failed Updates	This filter identifies all anti-virus update events (based on the Update Events filter), where the Category Outcome is Failure.	Filter	ArcSight Foundation/Common/Anti-Virus
Infected Systems	This query identifies data matching the AV - Found Infected filter where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus/Top Infected Systems

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Failed Anti-Virus Updates	This query identifies the device vendor, device product, target zone name, target host name, target address, and time (EndTime) from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus
Failed Anti-Virus Updates Chart	This query identifies the target zone name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/Anti-Virus
Virus Activity by Hour	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Foundation/Common/Anti-Virus/Virus Activity by Time
Top Zones with Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success, and the Category Significance starts with /Informational. The query returns the zone and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success, and the Category Significance starts with /Informational. The query returns the priority, vendor information, host information, error name, and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors
Update Summary Chart	This query identifies the target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus
Top Infected Systems	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus/Top Infected Systems
Top Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success, and the Category Significance starts with /Informational. The query returns the error name and the number of times the error occurred.	Query	ArcSight Foundation/Common/Anti-Virus/Errors

**Resources that Support the Anti-Virus Activity and Status Group, continued**

Resource	Description	Type	URI
Update Summary	This query identifies the target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Anti-Virus
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Two Charts One Table Landscape	This template is designed to show two charts and a table. The orientation is landscape.	Report Template	ArcSight System/2 Charts/With Table

## Attack Rates

The Attack Rates resources provide information about changes in attack activity by either service or target zone. The reports are driven by moving average data monitors. The dashboards display the appropriate data monitors for a view of the areas (services and target zones), to assist in determining whether the network is being attacked in a general sense, or if the attacks focus on specific network areas.

The following device types can supply events that apply to the Attack Rates resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Attack Rates Resource Group

The Attack Rates resource group requires the following configuration for your environment.

Enable the following trends:

- **Prioritized Attack Counts by Target Zone**—This trend is used by the Prioritized Attack Counts by Target Zone - Last 24 Hours report.
- **Prioritized Attack Counts by Service**—This trend is used by the Prioritized Attack Counts by Service - Last 24 Hours report.

## Attack Rates Resources

The following table lists all the resources in the Attack Rates group.

### Resources that Support the Attack Rates Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Attack Rates by Zones	This dashboard provides a broad overview of the attack rates in target zones and attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Top 10 Attack Rate Statistics by Service	This dashboard provides a top ten view of the attack rates by service and includes the target services (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Customer Attack Rates by Service	This dashboard provides an overview of the attack rates by service and includes the target service (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones. The overview is broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/
Top 10 Customer Attack Rate Statistics by Service	This dashboard shows a top ten view of the attack rates by service. The view includes the target services (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones. Each area is also broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/
Top 10 Customer Attack Rate Statistics by Service and Zones	This dashboard shows a top ten view of the attack rates by service. The dashboard shows the target services (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones. The overview is broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/
Top 10 Attack Rate Statistics by Zones	This dashboard provides a top ten view of the attack rates in target zones and attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attack Rates by Service and Zones	This dashboard displays an overview of the attack rates by service and includes the target service (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Customer Attack Rates by Service and Zones	This dashboard provides an overview of the attack rates by service and includes the target service (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones. Each area is also broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/
Top 10 Attack Rate Statistics by Service and Zones	This dashboard provides a top ten view of the attack rates by service and includes the target services (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Customer Attack Rates by Zones	This dashboard displays a broad overview of the attack rates in target zones and attacker zones. Each zone is also broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/
Top 10 Customer Attack Rate Statistics by Zones	This dashboard shows a top ten view of the attack rates in target zones and attacker zones. Each zone is also broken down by customer.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attack Rates by Service	This dashboard provides an overview of the attack rates by service and includes the target service (defined as the service name and port), the target services broken down by target zones, and the target services broken down by attacker zones.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Target Zone - Last 24 Hours	This report displays each target zone with counts of the events separated by priority. A table shows the event counts for each zone, subtotaled for each zone, and a total for all zones.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Service - Last 24 Hours	This report displays the target services by priority and the associated number of attack events for the previous day. The service displayed is a combination of the transport protocol, the application protocol, and the port number. A detailed table shows each target service and the number of attack events associated with the target service by priority for the same time period.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Trend: Prioritized Attack Counts by Service - Last 24 Hours	This report displays the target zones and the associated number of service events per hour. A table shows each target zone and the number of attack events associated with the target zone by hour and priority.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours	This report displays the target zones and the associated number of attack events per hour. A table shows each target zone and the number of attack events associated with the target zone by hour and priority.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
<b>Library Resources</b>			



**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attack Rates by Targeted Zone	This data monitor follows the possible attack counts for up to 20 target services by target zones (service here is defined as the service name and port), at five minute intervals over an hour. The data monitor send alerts at no more than ten minute intervals. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Attack Rates by Zone/
Attack Rates by Service	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Attack Rates by Service/
Attacker Zones by Service and Customer	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by attacker zone, at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Customer Attack Rates by Service and Zones/
Attack Rates by Service and Customer	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Customer Attack Rates by Service/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attack Rates by Attacker Zone and Customer	This data monitor follows the possible attack counts for up to 20 target services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Customer Attack Rates by Zone/
Top 10 Targeted Zones by Service	This data monitor follows the possible attack counts for the top ten targeted zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The data monitor refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Top 10 Attack Rate Statistics by Service and Zones/
Top 10 Attacker Zones by Service	This data monitor follows the possible attack counts for the top ten targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Top 10 Attack Rate Statistics by Service and Zones/
Targeted Zones by Service and Customer	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by target zone, at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Customer Attack Rates by Service and Zones/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Top 10 Targeted Zones by Service and Customer	This data monitor follows the possible attack counts for the top ten targeted zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Top 10 Customer Attack Rate Statistics by Service and Zones/
Top 10 Targeted Zones by Customer	This data monitor follows the possible attack counts for the top ten targeted services by targeted zones (service here is defined as the service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Top 10 Customer Attack Rate Statistics by Zones/
Attack Rates by Attacker Zone	This data monitor follows the possible attack counts for up to 20 target services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. The data monitor send alerts at no more than ten minute intervals. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Attack Rates by Zone/
Top 10 Attacked Services	This data monitor follows the possible attack counts for the top ten attacker zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Top 10 Attack Rate Statistics by Service/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attack Rates by Targeted Zone and Customer	This data monitor follows the possible attack counts for up to 20 target services by target zones (service here is defined as the service name and port), at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Customer Attack Rates by Zone/
Top 10 Attacker Zones	This data monitor follows the possible attack counts for the top ten targeted services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Top 10 Attack Rate Statistics by Zone/
Top 10 Attacker Zones by Service and Customer	This data monitor follows the possible attack counts for the top ten attacker zones and targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Top 10 Customer Attack Rate Statistics by Service and Zones/
Top 10 Targeted Zones	This data monitor follows the possible attack counts for the top ten targeted services by targeted zones (service here is defined as the service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Top 10 Attack Rate Statistics by Zone/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Attacker Zones by Service	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by attacker zone, at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Attack Rates by Service and Zones/
Top 10 Targeted Services by Customer	This data monitor follows the possible attack counts for the top ten targeted services (service here is defined as the transport protocol, service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Top 10 Customer Attack Rate Statistics by Service/
Targeted Zones by Service	This data monitor follows the possible attack counts for up to 20 target services (service here is defined as the transport protocol, service name and port) by target zone, at five minute intervals over an hour. The data monitor sends alerts at no more than ten minute intervals. The display refreshes every 30 seconds.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/Attack Rates by Service and Zones/
Top 10 Attacker Zones by Customer	This data monitor follows the possible attack counts for the top ten targeted services by attacker zones (service here is defined as the service name and port), at five minute intervals over an hour. The display refreshes every 30 seconds. The services are also broken down by customer.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/By Customer/Top 10 Customer Attack Rate Statistics by Zones/
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Possible Attack Events	This filter retrieves events in which the category significance is Compromise, Hostile or Suspicious. Note: There is no restriction on whether the target is an internal or external system.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attack Rates/
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Target Port is not NULL	This filter identifies if an event has an entry for the Target Port field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Prioritized Attack Counts by Service - Last Hour	This query identifies the service (the Service Variable, defined here as the transport name/service name: port) and priority, and sums the aggregated event count from events matching the Possible Attack Events filter over the last hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Service Query on Trend	This query identifies the hour, service name (Application Protocol Name/Transport Protocol Name: Target Port), and priority, and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend identifies the hour and target zone name, and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Prioritized Attack Counts by Target Zone - Last Hour	This query identifies the target zone name and priority, and Sums the aggregated event count from events matching the Possible Attack Events filter over the last hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/
Attack Counts by Service Query on Trend	This query on the Prioritized Attack Counts by Service trend identifies the hour and service name (Application Protocol Name/Transport Protocol Name: Target Port), and sums the number of events for that service for the Trend: Prioritized Attack Counts by Service - Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Target Zone Query on Trend	This query on the Prioritized Attack Counts by Target Zone trend identified the hour, target zone name, and priority and sums the number of events for that service for the Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Target Zone - Trend	This query populates the Prioritized Attack Counts by Target Zone trend. The query identifies the hour, target zone name, and priority and Sums the aggregated event count. The hour is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/Trend Queries/

**Resources that Support the Attack Rates Group, continued**

Resource	Description	Type	URI
Prioritized Attack Counts by Service - Trend	This query populates the Prioritized Attack Counts by Service trend. The query identifies the hour, service (a variable based on the service name or application protocol, the transport protocol, and the port; for example: HTML/TCP:80), and priority and sums the aggregated event count. The hour is used so that the data can be plotted based on the hour in which the event occurred, not the trend timestamp (the time the event data was stored in the trend).	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/Trend Queries/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Prioritized Attack Counts by Target Zone	This trend contains data selected by the query Prioritized Attack Counts by Target Zone - trend, which selects the hour, target zone, and priority and sums the aggregated event count. The hour is used so that the data can be plotted based on the hour in which the event occurred. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/
Prioritized Attack Counts by Service	This trend contains data selected by the query Prioritized Attack Counts by Service - Trend, which identifies the hour, service (a variable based on the service name or application protocol, transport protocol, and port; for example: HTML/TCP:80), and priority and sums the aggregated event count. The hour is used so that the data can be plotted based on the hour in which the event occurred. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/Attack Rates/



## Attackers

The Attackers resources provide statistics about attackers (such as reporting device, target host, target port, and ArcSight priority), views of attackers (by attacker port and, when available, by protocol), and statistics about attackers by using top and bottom 10 lists. The bottom 10 lists can be useful for tracking the attackers who are trying to avoid detection by the low-and-slow method (low volume over a long period of time).

The following device types can supply events that apply to the Attackers resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Attackers Resources

The following table lists all the resources in the Attackers group.

### Resources that Support the Attackers Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Target Counts by Attacker Port	This report displays the attacker port, target zone name, target address, and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Denied Outbound Connections by Port	This report shows a summary of the denied outbound traffic by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Top Users by Average Session Length	This report shows duration information about VPN connections for each user. A summary of the top VPN connection duration by user is provided. Details of the connection durations for each user are also provided, including minimum, average, maximum, and total connection minutes. Also included are details of connections that are open at the time the report is run.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/VPN/
Denied Outbound Connections per Hour	This report shows a summary of the denied outbound traffic per hour. A chart shows the total number of denied connections per hour for the previous day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Attacker Counts by Attacker Port	This report displays the attacker port, attacker zone name, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Connection Counts by User	This report shows count information about VPN connections for each user. A summary of the top users by connection count is provided. Details of the connection counts for each user are also provided, including connection count and the systems accessed.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/VPN/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Top N Attacker Details	This report displays the priority, attacker zone name, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/
Top Attacker Ports	This report displays the transport protocol, attacker port, and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Attacker Counts By Target	This report displays the attacker zone name, attacker address, the event name, and the count of attack events where the category significance starts with Compromise or Hostile, for the target zone and address specified in the parameters.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Denied Inbound Connections per Hour	This report shows a summary of the denied inbound traffic per hour. A chart shows the total number of denied connections per hour for the previous day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Top Attackers	This report displays a chart of the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/
Bottom N Attackers	This report displays a chart showing the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile, in ascending order of their event count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/
Denied Outbound Connections by Address	This report shows a summary of the denied outbound traffic by local address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Attacker Counts by ArcSight Priority	This report displays a table with the priority, attacker zone name, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Denied Inbound Connections by Address	This report shows a summary of the denied inbound traffic by foreign address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Top Alert Sources	This report shows the top IDS and IPS alert sources per day. A chart shows the top ten IDS and IPS alert source IP addresses. A table shows the top alert source IP addresses and zones, as well as the device vendor and product of the reporting device.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/IDS/
Attacker Port Counts	This report displays the attacker port, event name, and the count of attack events (the category significance starts with Compromise or Hostile).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Top N Attack Sources	This report displays the attacker zone name and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/
Attacker Counts by Device	This report displays a table with the device zone name, device address, attacker zone name, attacker address, and the count of attacker events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Attacker Counts by Target Port	This report displays the target port, attacker zone name, attacker address, and the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Bottom N Attack Sources	This report displays the attacker zone name and a sum of the count of attack events where the category significance starts with Compromise or Hostile.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/
Denied Inbound Connections by Port	This report shows a summary of the denied inbound traffic by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
<b>Library - Correlation Resources</b>			
Suspicious Communication From Attacked Target	This rule detects suspicious communication from an attacked target. The rule triggers when the attacker address and zone is on a Compromised Target or Untrusted attacker active list, and the attacker translated address and zone are on the Compromised Target active list; or whenever the target address and zone is in the Hostile or Suspicious Attacker active list. On the first event, agent severity is set to high and the attacker address is added to the Suspicious active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Attack From Suspicious Source	This rule detects attacks originating from a source categorized as suspicious or untrusted and does not belong to Attackers/Trusted active list. The rule triggers when an event originating from a source belonging to a suspicious or untrusted active list but not to the Attackers/Trusted active list has a category significance of Hostile and Compromise. On the first event, the source address is added to the Hostile active list and the event severity is set to high.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/
Probable Successful Attack - Probable Redirect Attack	This rule detects an exploit on a specific resource. It correlates two events: Attack_Redirection, which monitors any redirection attempt, and Attacks, which looks for recon, hostile, compromise, or suspicious events. The rule triggers when the Attack_Redirect event ends before the Attack event and the target is redirected to attacker zone (whenever there is a redirection before an attack). The rule does not trigger if the attacker is listed on a trusted list. On the first event, the attacker is added to the Hostile active list and the target to the Comprised active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - Information Leak	This rule detects information leaks. The rule correlates two events: File_access, which monitors any attempt to information leak or a successful information leak, and Access_success, which monitors successful access to a file. The rule triggers when the File_access event ends before the Access_success event (whenever a file is stolen and then accessed). The rule does not trigger if the attacker is on a trusted list. On the first event, the attacker is added to the Hostile list and the target to the Hit list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/
Probable Successful Attack - Repetitive Exploit Events	This rule detects a repetitive exploit attempt by the same attacker to the same target. The rule monitors events categorized as exploits coming from an attacker that is not on the Trusted Attackers active list. The rule triggers when three events occur within two minutes. On the first threshold, agent severity is set to high, the category significance is set to Hostile, and the category outcome is set to Attempt.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/



**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - Execute	This rule detects the creation, execution, or start of a specific resource. The rule correlates two events: Execute, which monitors successful resource starts, service creation or execution and file creation, and Execute_attack, which occurs whenever there is an attempt to execute a command on an operating system, service, or application. The rule triggers when the Execute_Attack event ends before the Execute event (when a resource is created, executed, or started because of a script execution). The rule does not trigger if the attacker is listed on a trusted list. On the first event, the attacker is added to the Hostile active list and the target is added to the Compromisedactive list. This rule is triggered by applications, services, or operating systems.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - System Configuration	This rule detects modifications in operating system configuration. It correlates two events: System_config, which monitors any successful modification of an operating system and Attack_configuration, which monitors configuration modifications that are categorized as hostile or informational warning. The rule triggers when the Attack_configuration event ends before the System_config event ( that is, whenever a modification of a system configuration is due to an attack). The rule does not trigger if an attacker is listed on a trusted list. On the first event, the attacker is added to the Hostile list and the target is added to the Compromised list. This rule is triggered by operating systems.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/
Suspicious Activity - Packet Manipulation	This rule detects any suspicious traffic anomaly. The rule triggers when three suspicious events occur within two minutes. On the first threshold, the attacker address is added to the Hostile active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - Exploit	This rule detects an exploit on a specific resource. The rule correlates two events: Buffer_Overflow, which monitors any exploit attempt and Service_Down, which monitors successful stop or deletion of a database, service, or application. The rule triggers when the Buffer_Overflow event ends before the Service_Down event (whenever a database, service, or application is stopped or deleted because of a Buffer_Overflow). The rule does not trigger if the attacker is listed on a trusted list. On the first event, the attacker is added to the Hostile list and the target is added to the Compromised list. This rule is triggered by applications, services, or databases.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/
High Number of IDS Alerts for Backdoor	This rule detects backdoor alerts from Intrusion Detection Systems (IDS). The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Firewall - Pass After Repetitive Blocks	This rule detects an attacker successfully passing through a firewall after having been blocked several times. The rule triggers when an attacker that belongs to an untrusted active list or the Repetitive Firewall Block List active list succeeds in going through the firewall. On the first event, the attacker address is added to the Suspicious List active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/Firewall/
Firewall - Repetitive Block - In Progress	This rule detects an attacker being blocked by the firewall repetitively. The rule monitors failure access. The rule triggers when ten events occur within three minutes from the same attacker. On the first threshold, the attacker address is added to the Repetitive firewall block list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/Firewall/
Suspicious Activity - Suspicious File Activity	This rule detects any failure that occurs with files between the same attacker/target pair. The rule triggers when four suspicious events occur within two minutes. On the first event, the attacker address is added to the Suspicious active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Multi Host Application Brute Force Logins	This rule detects brute force login attempts from different hosts using the same user name. It detects login attempts or failures from sources not listed on a trusted active list. The rule triggers after five occurrences from different hosts using the same user name within two minutes. On the first threshold, a correlation event is triggered that is caught by the Compromise - Attempt rule, which adds the attacker address to the Suspicious active list. The conditions require that the attacker address and zone are present, and that the generator ID (the rule's Resource ID) is not the same as this rule's generator ID.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - DoS	This rule detects a DoS attack against a specific service. The rule correlates two events: Attack_DoS, which is an attempt to a DoS attack, and Service, which occurs whenever an application is stopped or deleted, or a communication failure occurs. The rule triggers when the Attack_DoS event ends before the Service event (whenever an application is stopped or deleted, or a communication failure occurs due to a DoS attack). The rule does not trigger if the attacker is listed in a trusted active list. The rule does also not trigger if the attacker is already on the Infiltrators list, or if the target is already on the Hit list or Compromised list. On the first threshold, a correlation event with the categories Significance = Compromise and Outcome = Success is set.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Application Brute Force Logins	This rule detects application brute force login attempts with the same user name from the same attacker. The rule detects occurrences of login attempts or failure from sources not listed on a trusted active list. The rule triggers after five occurrences from the same attacker within two minutes. On the first threshold, a correlation event is triggered that is caught by the Compromise - Attempt rule, which adds the attacker address to the Suspicious active list. The conditions require that the attacker address and zone are present, and that the generator ID (the Resource ID in the rule) is not the same as the generator ID for this rule.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/
Firewall - High Volume Accepts	This rule monitors the moving average of accepts per zone. The rule triggers when the monitoring threshold drastically changes (50%). The monitoring threshold and the moving average parameters are determined by the Moving Average dashboard for the firewall accept. This rule triggers when there is a 50% change in firewall accepts.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Attack - Script Attack	This rule detects multiple executions of scripts, (HTTP, CGI, and so on) that have the same event name, attacker address, and target address within a short period of time. The rule monitors any attempts to start or execute a script that target an application, a service, or an operating system. The rule triggers when ten events occur within one minute with the same event name, attacker address, and target address. On the first threshold, the attacker address is added to the Hostile active list and the target address is added to the Hit active list. Note: This rule does not trigger when running in Turbo Mode Fastest.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/
Notify on Successful Attack	This rule detects successful attacks. This rule looks for high priority ( $\geq 8$ ) successful attacks for which the attacker is not in the Attackers/Trusted list. This rule only requires one such event, and the time frame is set to ten minutes. After this rule is triggered, a notification is sent to the CERT team. The action to create a new case is available, but is disabled by default.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/



**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Probable Successful Attack - Brute Force	This rule detects brute force attack events and correlates it with a successful authentication event where the attack source and attacked target are the same, using the same target user ID. The rule triggers when five events occur within two minutes with the same attacker address and target address. On the first threshold, the user name is added to the Compromised User Accounts active list, and a correlation event is triggered that will be processed by the Compromise - Success rule. Note: This rule does not trigger when running in Turbo Mode Fastest.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/
<b>Library Resources</b>			
Hit List	This Active List contains hosts targeted by a potential attacker.	Active List	ArcSight System/Targets
Hostile List	This Active List contains hosts that have been attempting attacks on systems.	Active List	ArcSight System/Threat Tracking
Suspicious List	This Active List contains hosts which have performed suspicious activity, either on the local system or over the network.	Active List	ArcSight System/Threat Tracking
Compromised List	This Active List contains hosts that may have been compromised by an attack.	Active List	ArcSight System/Threat Tracking
Compromised User Accounts	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Infiltrators List	This Active List contains hosts which have compromised (infiltrated) a system.	Active List	ArcSight System/Threat Tracking
Brute Force Login Attempt	This resource has no description.	Active List	/All Active Lists/ArcSight Core Security/Security Activity
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight System/Tuning
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	Active List	ArcSight System/Attackers
Repetitive Firewall Block List	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Dark	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Base events.	Filter	/All Filters/ArcSight Core Security/IDS-IPS Monitoring
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Top 10 Attackers	This report shows the top ten attackers.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/IDS/
Attacker Counts by Target Port	This query identifies the target port, attacker zone name, attacker address, and the count of events where the target port is not null and the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Top Attacker Ports	This query identifies the transport protocol, attacker port, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Top 10 Attackers	This query identifies the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom 10/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Bottom 10 Attackers	This query identifies the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers using different attacks are not split by the attacker address or the attack type.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom 10/
Top Alert Sources	This query identifies the count of IDS and IPS alerts by source address, zone, device vendor, and device product.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/IDS/
Denied Inbound Connections per Hour	This query identifies the count of denied inbound connections per hour for each source zone.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Top 10 Attacker Details	This query identifies the priority, attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom 10/
Closed VPN Connection Durations	This query returns the user ID and the minimum, average, maximum, and total durations (in minutes) for all user IDs with closes or terminated VPN sessions in the User VPN Sessions list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/Connection Durations by User/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Attacker Port Counts	This query identifies the attacker port, event name, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Denied Inbound Connections by Port	This query identifies the count of denied inbound connections by destination port.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Top 10 Attack Sources	This query identifies the attacker zone name and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attacks from within a zone are not split by the attacker address or the attack type.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom 10/
Attacker Counts by ArcSight Priority	This query identifies the priority, attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Users by Connection Count	This query identifies VPN events where the category behavior is /Access/Start, /Authentication/Verify, or /Authorization/Verify, with user information available, returning the user and host information, and the number of VPN connections.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/Connection Counts by User/
Denied Outbound Connections by Address	This query identifies the count of denied outbound connections by local address (source zone, address, and hostname).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Denied Outbound Connections by Port	This query identifies the count of denied outbound connections by destination port.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Attacker Counts By Target	This query identifies the attacker zone name, attacker address, the event name, and the count of events where the category significance starts with Compromise or Hostile for the target information given in the parameters.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Attacker Counts by Device	This query identifies the device zone name, device address, attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Top VPN Connection Durations	This query identifies the user ID and the average duration from the User VPN Sessions list, sorted by the top duration.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/Connection Durations by User/
Denied Outbound Connections per Hour	This query identifies the count of denied outbound connections per hour for each source zone.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Denied Inbound Connections by Address	This query identifies the count of denied inbound connections by foreign address (source zone, address, and hostname).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Target Counts by Attacker Port	This query identifies the attacker port, target zone name, target address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Top Users by Connection Count	This query identifies VPN events in which the Category Behavior is /Access/Start, /Authentication/Verify, or /Authorization/Verify, with user information available, returning the number of VPN connections per user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/Connection Counts by User/
Attacker Counts by Attacker Port	This query identifies the attacker port, attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Port or Protocol/
Denied Outbound Connections per Hour (Chart)	This query identifies the count of denied outbound connections per hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Denied Inbound Connections per Hour (Chart)	This query identifies the count of denied inbound connections per hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/



**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
Bottom 10 Attack Sources	This query identifies the attacker zone name and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attacks from within a zone are not split by the attacker address or the attack type.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom 10/
Users with Open VPN Connections	This query identifies the user ID and the VPN device for each user in the User VPN Sessions list where the user entry has not been terminated (logged out or timed out) or expired (by default).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/Connection Durations by User/
Chart and 2 Tables Portrait	This template is designed to show one chart and two tables. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With 2 Tables
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

**Resources that Support the Attackers Group, continued**

Resource	Description	Type	URI
User VPN Sessions	This session list tracks VPN user session starts and stops (or terminations), for purposes of tracking user session durations. The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	Session List	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/

## Business Impact Analysis

The Business Impact Analysis resources provide information about which business areas are the victims of the most attack activity.

The following device types can supply events that apply to the Business Impact Analysis resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Business Impact Analysis Resource Group

Categorize all assets that have a business role in your environment with the **Business Role** asset category. For more information about categorizing assets, refer to ["Categorizing Assets" on page 11](#).

## Business Impact Analysis Resources

The following table lists all the resources in the Business Impact Analysis group.

### Resources that Support the Business Impact Analysis Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Business Roles - Last Hour	This active channel shows events received during the last hour. The active channel includes a sliding window that displays the last hour of event data, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Business Role. The Business Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis and uses the Business Impact Analysis field set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).	Active Channel	ArcSight Foundation/Intrusion Monitoring/Business Impact Analysis/Business Roles/

**Resources that Support the Business Impact Analysis Group, continued**

Resource	Description	Type	URI
Business and Data Roles	This active channel shows events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data, showing an overview of hostile and compromise events relating to assets within the Business Role, Data Role, or Classification categories. The events match the Targeted Business Impact Analysis filter. The Business Role, Data Role, and Classification categories are sub-categories of /All Asset Categories/Site Asset Categories/Business Impact Analysis. The active channel uses the Business Impact Analysis field set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).	Active Channel	ArcSight Foundation/Intrusion Monitoring/Business Impact Analysis/
Business Roles - Today	This active channel shows events received since midnight today. The active channel includes a sliding window that displays event data since midnight, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Business Role. The Business Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis and uses the Business Impact Analysis field set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).	Active Channel	ArcSight Foundation/Intrusion Monitoring/Business Impact Analysis/Business Roles/
Data Roles - Today	This active channel shows events received since midnight today. The active channel includes a sliding window that displays event data since midnight, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Data Role. The Data Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis and uses the Business Impact Analysis field set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).	Active Channel	ArcSight Foundation/Intrusion Monitoring/Business Impact Analysis/Data Roles/

**Resources that Support the Business Impact Analysis Group, continued**

Resource	Description	Type	URI
Data Roles - Last Hour	This active channel shows events received during the last hour. The active channel includes a sliding window that displays the last hour of event data, showing events matching the Targeted Business Impact Analysis filter, with the further restriction that the target asset has a Data Role. The Data Role category is a sub-category of /All Asset Categories/Site Asset Categories/Business Impact Analysis and uses the Business Impact Analysis field set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).	Active Channel	ArcSight Foundation/Intrusion Monitoring/Business Impact Analysis/Data Roles/
Business Role - Successful Attacks	This report shows the role and the sum of the aggregated event count for events with target asset IDs in the All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role asset category, that match the Attack Events filter and have a category outcome of Success.	Report	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Business Roles/
Business Role - Attempted Attacks	This report shows the role and the sum of the aggregated event count for events with target asset IDs in the All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role asset category, that match the Attack Events filter and have a category outcome that is not success.	Report	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Business Roles/
<b>Library Resources</b>			
Data Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Business Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis

**Resources that Support the Business Impact Analysis Group, continued**

Resource	Description	Type	URI
Business Impact Analysis	<p>This field set includes:</p> <p>End Time</p> <p>Business Role</p> <p>Data Role</p> <p>Attacker Zone Name</p> <p>Target Host Name</p> <p>Category Significance</p> <p>Category Outcome</p> <p>Priority</p>	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Targeted Business Impact Analysis	<p>This filter detects hostile &amp; compromise events relating to target assets within the Business Role, Data Role or Classification categories. The events match:</p> <ul style="list-style-type: none"> <li>- Non-ArcSight Internal Event</li> <li>- Target asset has a Business Impact Analysis Category</li> <li>- Priority &gt; 5</li> <li>- Category Significance StartsWith /Compromise or /Hostile</li> </ul> <p>The Business Role, Data Role and Classification categories are sub-categories of /All Asset Categories/Site Asset Categories/Business Impact Analysis.</p>	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types

**Resources that Support the Business Impact Analysis Group, continued**

Resource	Description	Type	URI
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
Successful Attacks	This filter detects events that have a significance of Compromise or Hostile, and an outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Business Role - Successful Attacks	This query returns the role and the sum of the aggregated event count for events with Target Asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role asset category, that match the Attack Events filter and have a category outcome of success.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Business Role/
Business Role - Attempted Attacks	This query returns the role and the sum of the aggregated event count for events with Target Asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role asset category, that match the Attack Events filter and have a category outcome that is not success.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Business Role/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## DoS

The DoS (Denial of Service) resources use moving average data monitors and categorized events with the technique set to /DoS to help determine when a DoS is taking place. The data monitors highlight high-volume activity that might result in a DoS. The categorized events (mostly from an IDS) can show DoS events that do not require exceeding bandwidth or processing limitations.

The following device types can supply events that apply to the DoS resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the DoS Resource Group

The DoS resource group requires the following configuration for your environment:

- Populate the **Event-based Rule Exclusions** active list with the events that you do not want to trigger rules.
- Enable the **Inbound DoS Events** trend. This trend is used by the **Trend: Inbound DoS Events - Yesterday** report.

## DoS Resources

The following table lists all the resources in the DoS group.

### Resources that Support the DoS Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			



**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
DoS Channel	This active channel shows events received during the last two hours and includes a sliding window that displays the last two hours of event data. The active channel uses its own filter to limit the view to Denial of Service related events where the Category Technique is /DoS, the Category Significance is /Compromise, the Category Outcome is /Success, and the event MatchesFilter(Internal Target) .	Active Channel	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Inbound Event Spikes	This dashboard includes several moving average data monitors that measure event activity looking for suspicious spikes in activity. Use these data monitors to determine if a Denial of Service attack is starting. The data monitors include activity reported by firewalls, activity related to the protected network, activity related to protected host, and activity related to the services on the protected network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/
Trend: Inbound DoS Events - Yesterday	This report displays the target zones and the associated number of DoS events per hour.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/
Inbound DoS Events - Yesterday	This report displays a 3D stacking bar chart showing each target zone with the counts of the DoS events separated by service. A detailed table follows the chart, with the DoS event counts for each zone subtotaled for each zone, with a total for all zones at the end.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/
<b>Library Resources</b>			

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight System/Tuning
ArcSight System Administration	This is a system administration asset category.	Asset Category	/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Inbound Event Spikes for Hosts	This data monitor sums the count of events constrained by the Inbound Events for Hosts filter. The data monitor checks up to ten hosts (zone/host, the ten most frequently accessed hosts) over thirty second intervals over a period of a half-hour. It sends an alarm event if the moving average changes by 300%. This data monitor detects sudden increases in request or access activity related to the protected hosts. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of ten or so packets with an average of one would be a false positive.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/Inbound Event Spikes/

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Inbound Event Spikes for Services	This data monitor sums the count of events constrained by the Inbound Events for Service filter. The data monitor checks up to 10 services (zone/address/port, the 10 most accessed hosts/services) over fifteen second intervals over a fifteen minute period. It sends an alarm event if the moving average changes by 300%. This data monitor detects sudden increases in activity related to services on the protected network. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of ten or so packets with an average of one would be a false positive.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/Inbound Event Spikes/

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Inbound Event Spikes for Networks	This data monitor sums the count of events constrained by the Inbound Events for Networks filter. The data monitor checks up to ten zones (the ten most frequently accessed zones) over one minute intervals over a period of an hour. It sends an alarm event if the moving average changes by 300%. This data monitor detects sudden increases in request or access activity related to the protected network. The alarm threshold is set high to detect significant spikes in the related event flow. The discard threshold is also set high (average 100 events per second) to filter out low event rates where an event spike of ten or so packets with an average of one would be a false positive.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/Inbound Event Spikes/
Firewall Accepts	This data monitor sums the count of events constrained by the Inbound Events for Networks filter. The data monitor checks up to five firewalls (the five firewalls reporting the most request or access activity) over five minute intervals over a period of an hour. It sends an alarm event if the moving average changes by 50%. This data monitor detects sudden increases in request or access activity related to the protected network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/Inbound Event Spikes/
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Firewall Accepts	This resource has no description.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Possible Attack Events	This filter retrieves events in which the category significance is Compromise, Hostile or Suspicious. Note: There is no restriction on whether the target is an internal or external system.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attack Rates/
Inbound Events for Service	This filter retrieves request or access events targeting internal services, with the exception of trusted attackers (approved internal vulnerability scanners) and ArcSight administrative assets.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Inbound Events for Networks	This filter retrieves request or access events targeting the network as a whole, with the exception of trusted attackers (approved internal vulnerability scanners) and ArcSight administrative assets.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Target Port is not NULL	This filter identifies if an event has an entry for the Target Port field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Successful Inbound DoS Events - Trend Filter	This filter identifies events that are related to successful Denial of Service attacks on internal targets, with the exception of trusted attackers (approved internal vulnerability scanners). This filter is used to select events by a query for a trend on Denial of Service attacks affecting the network, but can also be used for filtering events for a standard event report (not a trend report).	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Base events.	Filter	/All Filters/ArcSight Core Security/IDS-IPS Monitoring
Target Asset has Asset Name	This filter is used by some of the query variables to determine if an event has an entry for the Target Asset Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Asset
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Inbound Events for Hosts	This filter retrieves request or access events targeting internal hosts on the network as a whole, with the exception of trusted attackers ( approved internal vulnerability scanners) and ArcSight administrative assets.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Foundation/Common/Device Class Filters
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Successful Inbound DoS Events Query on Trend	This query on the Inbound DoS Events trend returns the target zone name, the target asset name (or its IP address), the service name (Application Protocol Name/Transport Protocol Name: Target Port), a timestamp and sums the number of Denial so Service events against the services on that asset during the time-period (hourly), for the Trend: Inbound DoS Events - Yesterday report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/
Successful Inbound DoS Events Last Hour	This query returns data for reporting the target zone name, the asset name (or IP address), the service name, and a summary of event counts. Note: The filter used is also used for a trend.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/DoS/
Successful Inbound DoS Events - Trend	This query returns data for reporting the target zone name, the asset name (or IP address), the service name and a summary of event counts. This data is used to populate the Inbound DoS Events trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/Trend Queries/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

**Resources that Support the DoS Group, continued**

Resource	Description	Type	URI
Inbound DoS Events	This trend contains data selected by the Successful Inbound DoS Events - Trend query, which selects the day, the service (a variable based on the service name or application protocol, the transport protocol, and the port such as HTML/TCP:80), the TargetAssetName (a variable using the host name, if available, or the IP address), and sums the aggregated event count. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/



## Environment State

The Environment State resources provide information about activity that reflects the state of the overall network, and provide details about applications, operating systems and services.

The following device types can supply events that apply to the Environment State resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Environment State Resources

The following table lists all the resources in the Environment State group.

### Resources that Support the Environment State Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Application Overview	This active channel shows events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data. The channel uses two filters to limit the view to application related events, non-ArcSight internal events, and events for internal applications excluding services.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Environment State/
Service Overview	This active channel shows events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data. The active channel uses two filters to limit the view to service related events, non-ArcSight internal events, and events for internal services.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Environment State/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Operating System Overview	This active channel shows events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data. The channel uses two filters to limit the view to operating system related events, non-ArcSight internal events, and events for internal operating systems.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Environment State/
Current Environment Status Overview	This dashboard shows an overview of the current environment based on application events, operating system events, and service events. There are two data monitors for each area, a moving average data monitor and a top ten events data monitor. Use this dashboard to view changes in network activity and see the most frequent events.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/
Trend: Top Application Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by application. A detailed table follows the chart, with each application and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Application/
Trend: Environment Status Events - Yesterday	This report displays four 3D stacked bar charts. The first chart shows each target zone with the event count trend for the network. The remaining charts show the application, operating system, or service event trends separated by zones.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Environment Status Events over the Last 24 Hours	This report displays several 3D stacked bar charts. The first chart shows each target zone with the event counts for the network. The remaining charts show the application, operating system, or service events separated by zones.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/
Trend: Top OS Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by operating system. A detailed table follows the chart, with each OS and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Operating System/
Top Service Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing the service status event counts by application. A detailed table follows the chart, with each service and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Service/
Top OS Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing the OS status event counts by operating system. A detailed table follows the chart, with each operating system and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Operating System/
Top Application Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing the application status event counts by application. A detailed table follows the chart, with each application and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Application/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Trend: Top Service Status Events over the Last 24 Hours	This report displays a 3D stacked bar chart showing each target zone with a trend of the event counts separated by service. A detailed table follows the chart, with each service and host in descending order by the event counts.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Service/
<b>Library Resources</b>			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Operating System	This is a site asset category.	Asset Category	Site Asset Categories
Service Event Counts	This data monitor sums the count of events constrained by the Events for Internal Services filter. The data monitor checks up to 20 Category Objects (the 20 most frequent events related to that object) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. This data monitor detects sudden increases or decreases in activity related to services on the protected network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/
Top 10 Application Events	This data monitor shows events constrained by the Events for Internal Applications excluding services filter. The data monitor checks 1,000 distinct events in five minute intervals over the period of an hour.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/
Top 10 Service Events	This data monitor displays events constrained by the Events for Internal Services filter. The data monitor checks 1,000 distinct events in five minute intervals over the period of an hour.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Application Event Counts	This data monitor sums the count of events constrained by the Events for Internal Applications excluding services filter. The data monitor checks up to 20 Category Objects/Category Device Groups (the 20 most frequent events related to that object/device) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. This data monitor detects sudden increases or decreases in activity related to applications on the protected network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/
Operating Systems Event Counts	This data monitor sums the count of events constrained by the Events for Internal Operating Systems filter. The data monitor checks up to 20 Category Objects/Category Device Groups (the 20 most frequent events related to that object/device) over five minute intervals over a two hour period. It sends an alarm event if the moving average changes by 50%. This data monitor detects sudden increases or decreases in activity related to operating systems on the protected network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/
Top 10 Operating System Events	This data monitor shows events constrained by the Events for Internal Operating Systems filter. The data monitor checks 1,000 distinct events in five minute intervals over the period of an hour.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Current Application Status Overview/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Status Overview	This field set includes: End Time, Name, Category Object, Category Device Group, Attacker Target, Priority, Device Vendor, and Device Product.	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Events for Internal Applications excluding services	This filter identifies events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to being in the Application category device group or being a Category Object of /Host/Application, but not a Category Object of /Host/Application/Service.	Filter	ArcSight Foundation/Intrusion Monitoring/Environment State/
Target Asset has OS Categorization	This filter identifies if the target in an event has an Asset Category within /Site Asset Categories/Operating System.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Asset
Target Object starts with Host Application	This filter identifies if an event Category Object is within /Host/Application.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Categories
Target Port is not NULL	This filter identifies if an event has an entry for the Target Port field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Target Asset has Asset Name	This filter is used by some of the query variables to determine if an event has an entry for the Target Asset Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Asset
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Events for Internal Services	This filter identifies events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to having a port set or being a Category Object of /Host/Application/Service.	Filter	ArcSight Foundation/Intrusion Monitoring/Environment State/
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Events for Internal Operating Systems	This filter identifies events that are not ArcSight internal events and that are related to an internal destination. The events are further limited to being in the Category Device Group /Operating System or being a Category Object of /Host/Operating System.	Filter	ArcSight Foundation/Intrusion Monitoring/Environment State/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Top Service Status Events on Trend	This query returns the target zone name, the trend type name (dvLabelName), and the time and sums the number of events for that zone in the time-range for the Top Service Status Events over the Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Service/
Top Service Status Events over the Last 24 Hours (Chart Query)	This query returns the data for reporting the target zone name, service name (a variable field), and a summary of the event counts for overview information in a report (a chart). This query uses the Events for Internal Services filter to limit events to those relating to services.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Service/
Top Status Events on Trend	This query returns the target zone name, the trend type (application, operating system, service), the time, and sums the number of events for that zone in the time-range for the Environment Status Events - Yesterday report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Application, OS and Service/
Top OS Status Events over the Last 24 Hours	This query returns the data for reporting the target zone name, operating system name (a variable field), the target asset name (another variable field), and a summary of the event counts for detailed information in a report (a table). This query uses the Events for Internal Operating Systems filter to limit events to those relating to Operating Systems.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Operating System/



**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Top Application Status Events on Trend	This query returns the target zone name, the trend type name (dvLabelName), the time, and sums the number of events for that zone in the time-range for the Top Application Status Events over the Last 24 Hours report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Application/
Environment Status Events - Trend	This query detects the data for reporting the target zone name, the time (expressed within a variable), the service, operating system or application name (another variable field), and a summary of the event counts for overview information to populate the trend Environment Status Events. This query uses the Events for Internal Operating Systems, Events for Internal Applications excluding services and Events for Internal Services filters to limit events to those relating to the network environment state.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Application, OS and Service/Trend Queries/
Top Application Status Events over the Last 24 Hours	This query returns the data for reporting the target zone name, application name (a variable field), the target asset name (another variable field), and a summary of the event counts for detailed information in a report (a table). This query uses the Events for Internal Applications excluding services filter to limit events to those relating to applications.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Application/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Top Operating System Status Events on Trend	This query returns the target zone name, the trend type name (dvLabelName), the time, and sums the number of events for that zone in the time-range for the Top OS Status Events over the Last 24 Hours report trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/Operating System/
Top Service Status Events over the Last 24 Hours	This query returns the data for reporting the target zone name, service name (a variable field), the target asset name (another variable field), and a summary of the event counts for detailed information in a report (a table). This query uses the Events for Internal Services filter to limit events to those relating to services.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Service/
Environment Status Events over the Last 24 Hours (Chart Query)	This query returns the data for reporting the target zone name, the target asset name (a variable field), and a summary of the event counts for overview information in a report (a chart). This query uses the Events for Internal Operating Systems, Events for Internal Applications excluding services and Events for Internal Services filters to limit events to those relating to the network environment state.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/
Top Application Status Events over the Last 24 Hours (Chart Query)	This query returns the data for reporting the target zone name, application name (a variable field), and a summary of the event counts for overview information in a report (a chart). This query uses the Events for Internal Applications excluding services filter to limit events to those relating to applications.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Application/

**Resources that Support the Environment State Group, continued**

Resource	Description	Type	URI
Top OS Status Events over the Last 24 Hours (Chart Query)	This query returns the data for reporting the target zone name, operating system name (a variable field), and a summary of the event counts for overview information in a report (a chart). This query uses the Events for Internal Operating Systems filter to limit events to those relating to Operating Systems.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Environment State/Operating System/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Four Charts Landscape	This template is designed to show four charts. The orientation is landscape.	Report Template	ArcSight System/4 Charts/Without Table
Environment Status Events	This trend collects summary counts of events, storing the target zone, the time, the service, application or operating system names, and a marker field that can be used by queries to extract data for any one or all of the related areas. This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Environment State/

## Login Tracking

The Login Tracking resources provide information about user logins.

The following device types can supply events that apply to the Login Tracking resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems
- Identity management systems
- VPNs

## Configuring the Login Tracking Resource Group

Populate the ArcSight System/Tuning/**User-based Rule Exclusions** active list with the users you want to exclude from certain rule conditions where the rule tracks user activity.

## Login Tracking Resources

The following table lists all the resources in the Login Tracking group.

### Resources that Support the Login Tracking Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Network Login Overview	This dashboard shows an overview of logins on network devices. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and the Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
VPN Login Overview	This dashboard shows an overview of VPN logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Identity Management Overview	This dashboard displays information reported by Identity Management devices, such as the top users by number of connections and authentication failures by source and destination.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Firewall Login Overview	This dashboard shows an overview of firewall logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Operating System Login Overview	This dashboard shows an overview of operating system logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Logins by User	This reports shows authentication successes from login attempts by user. A chart shows the top users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Device SNMP Authentication Failures	This report shows summaries of SNMP authentication failures by device or by user. A table details the failed user SNMP authentication attempts for the devices. Two charts give an overview of the users or devices with the most SNMP authentication failures. Use this report to help determine if SNMP accounts are targets of brute force attacks and which devices are exhibiting the most SNMP authentication failure activity.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Failed Login Attempts	This report shows the count of authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Failed Logins by Destination Address	This report shows authentication failures from login attempts by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Connection Durations by User	This report shows duration information about VPN connections for each user. A summary of the top VPN connection duration by user is provided. Details of the connection durations for each user are also provided, including minimum, average, maximum, and total connection minutes. Also included are details of connections that are currently open at the time the report is run. By default, this report shows user VPN duration information for the previous day.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Windows Events	This report displays a table showing the event information, reported by any Microsoft operating system.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Connection Counts by User	This report shows count information about connections for each user reported by Identity Management devices. A summary of the top users by connection count is provided.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
User Activity	This report displays a table showing user activity information.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Successful Logins by Source Address	This report shows authentication successes from login attempts by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Login Errors by User	This report shows a summary of the operating system login errors by username. A chart shows the top ten users with failed logins. A table shows details of the failed logins for each username (time, event name, source, destination).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/



**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Top Hosts by Number of Connections	This report shows a summary of the number of connections by the top hosts in a chart. By default, the chart shows the number of connections by host for the previous day.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
<b>Library - Correlation Resources</b>			
User Session (Administrative User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Cisco Secure ACS.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
User Session (Accounting User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
User Session (Normal User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
User Session (Accounting User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
User Session (Administrative User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Cisco Secure ACS.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
User VPN Session Stopped	This rule detects VPN user session stop (or terminate) events, defined as a VPN access stop event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
User Session (Normal User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/

### Resources that Support the Login Tracking Group, continued

Resource	Description	Type	URI
User VPN Session Started	This rule detects VPN user session start events, defined as a VPN access start event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
<b>Library Resources</b>			
Last 10 Failed Login Events	This data monitor shows the last ten failed VPN logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/VPN Login Overview/
Top Users by Login Activity	This data monitor shows the users with the most VPN login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/VPN Login Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed operating system logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System Login Overview/
Top Users by Login Activity	This data monitor shows the users with the most network login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful logins on network devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Authentication Failures by Source	This data monitor displays the source information of failed authentication attempts within five-minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/Identity Management Overview/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Top Users by Login Activity	This data monitor shows the users with the most operating system login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System Login Overview/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top ten users with failed logins on network devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Login Results	This data monitor shows the number of VPN logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/VPN Login Overview/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Login Results	This data monitor shows the number of operating system logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top ten users with failed operating system logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System Login Overview/
Authentication Failures by Destination	This data monitor displays the destination information of failed authentication attempts within five-minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/Identity Management Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful operating system logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System Login Overview/

### Resources that Support the Login Tracking Group, continued

Resource	Description	Type	URI
Login Results	This data monitor shows the number of logins on network devices (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful VPN logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/VPN Login Overview/
Top Users by Connection Count	This data monitor shows the top users by the number of connections in five-minute intervals for the last hour, as reported by Identity Management devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/Identity Management Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed logins on network devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top ten users with failed VPN logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/VPN Login Overview/
ActingUser	This variable returns the AttackerUser, if known, or the TargetUser, if that is the only user information available within the event. The format is the same as the AttackerUser or TargetUser variables.	Global Variable	ArcSight Foundation/Variables Library/User Information

### Resources that Support the Login Tracking Group, continued

Resource	Description	Type	URI
AttackerUser	This variable displays the attacker user name. If the attacker user name is unavailable, the variable displays the attacker user ID. If neither field is available, the variable displays unknown.	Global Variable	ArcSight Foundation/Variables Library/User Information
TargetUser	This variable displays the target user name. If the target user name is unavailable, the variable displays the target user ID. If neither field is available, the variable displays unknown.	Global Variable	ArcSight Foundation/Variables Library/User Information
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight System/Event Field Sets/Active Channels
VPN Events	This filter identifies events in which the category device group is VPN.	Filter	ArcSight Foundation/Common/Device Class Filters
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Foundation/Common/Device Class Filters
Login Events	This filter identifies events where the category behavior is /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Identity Management Connection Start Events	This filter identifies events where an Identity Management system has seen an access start event with valid user information.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Failed Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/
VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
Failed Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
All Events	This filter matches all events.	Filter	ArcSight System/Core
Successful Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
Failed Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify, the category outcome is Failure, and the category object starts with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify, the category outcome is Success, and the category object starts with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/
Attacker User ID is NULL	This filter identifies events where the Attacker User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Foundation/Common/Device Class Filters
Attacker User Name is NULL	This filter identifies events where the Attacker User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Failed Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/
Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify and the category device group starts with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/
Database Events	This filter identifies events in which the category object is /Host/Application/Database.	Filter	ArcSight Foundation/Common/Device Class Filters
Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/
Successful VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/



**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Attacker User Name and ID are NULL	This filter identifies events in which the Attacker User Name and Attacker User ID are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Failed Identity Management Login Attempts	This filter identifies events where an authentication attempt failed.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	Filter	ArcSight Foundation/Common/Device Class Filters
Operating System Events	This filter identifies events in which the category device group is Operating System.	Filter	ArcSight Foundation/Common/Device Class Filters
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User
Successful Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Successful Logins by Source Address	This report shows authentication successes from network login attempts by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Failed Login Attempts	This report shows the count of authentication failures from login attempts reported by identity management systems by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall connections by the top hosts. By default, a chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Logins by Source Address	This report shows authentication successes from operating system login attempts by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Successful Logins by User	This report shows authentication successes from login attempts by user reported by identity management systems. A chart shows the top users with successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Top Hosts by Number of Connections	This report shows a summary of the number of network connections by the top hosts. By default, a chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Successful Logins by User	This report shows authentication successes from network login attempts by user. A chart shows the top users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Failed Logins by User	This report shows authentication failures from network login attempts by user. A chart shows the top ten users with failed login attempts. A table shows details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by Destination Address	This report shows authentication failures from login attempts reported by identity management systems by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Login Event Audit	This report shows all the successful and failed firewall login events in a table, sorted chronologically. This is a focused report based on the Login Events report.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from operating system login attempts by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from VPN login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Failed Login Attempts	This report shows the count of operating system authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Successful Logins by Destination Address	This report shows authentication successes from network login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by User	This report shows authentication failures from VPN login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Successful Logins by Destination Address	This report shows authentication successes from login attempts reported by identity management systems by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Successful Logins by User	This report shows a summary of the successful operating system logins by username. A chart shows the top ten usernames with successful logins. A table shows details of the successful logins for each username (time, source, destination).	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by Destination Address	This report shows authentication failures from VPN login attempts by destination address. A chart shows the top ten destination addresses with failed login attempts. a table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Successful Logins by Destination Address	This report shows authentication successes from operating system login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Failed Logins by Source Address	This report shows authentication failures from network login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Successful Logins by Source Address	This report shows authentication successes from VPN login attempts by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Database/
Failed Logins by Source Address	This report shows authentication failures from login attempts reported by identity management systems by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Login Event Audit	This report shows all the successful and failed operating system login events in a table, sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Top Hosts by Number of Connections	This report shows a summary of the number of VPN connections by the top hosts in a chart. By default, the chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Failed Logins by User	This report shows a summary of the failed operating system logins by username. A chart shows the top ten usernames with failed logins. A table shows details of the successful logins for each username (time, source, destination).	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/



**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Login Event Audit	This report shows all the successful and failed VPN login events in a table, sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Successful Logins by Source Address	This report shows authentication successes from login attempts reported by identity management systems by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Login Event Audit	This report shows all the successful and failed network login events in a table sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Failed Logins by Source Address	This report shows authentication failures from operating system login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Successful Logins by User	This report shows authentication successes from VPN login attempts by user. A chart shows the top users with successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Failed Logins by User	This report shows authentication failures from login attempts by user reported by identity management systems. A chart shows the top users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Failed Logins by Destination Address	This report shows authentication failures from network login attempts by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from VPN login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/VPN/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
User Activity	This query returns events in which source user ID, source user name, destination user ID, or destination user name is not NULL.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/
Users with Open Connections	This query returns the user ID and the Identity Management device for each user in the User Sessions list where the user entry has not been terminated (logged out or timed out) or expired (by default).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Windows Events	This query returns events reported by the Microsoft operating system.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Users by Connection Count	This query returns events in which the category behavior is /Access/Start, /Authentication/Verify or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Top Connection Durations	This query returns the user ID and average duration from the User Identity Management Sessions list and sorts them by the top duration.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Failed Login Attempts	This query returns all authentication failures from login attempts.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Top Users by Connection Count	This query returns events in which the Category Behavior is /Access/Start, /Authentication/Verify or /Authorization/Verify. If user information is available, the query returns the number of connections per user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Login Errors by User	This query returns operating system login errors. The query returns the user name, event name, source and destination addresses, hostnames, and zones.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Login Errors by User (Chart)	This query returns the count of operating system login errors by username.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Operating System/
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Closed Connection Durations	This query returns the user ID and the minimum, average, maximum, and total durations (in minutes) for all user IDs with closed or terminated sessions in the User Sessions list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Identity Management/
Failed Login Attempts (Chart)	This query returns the count of authentication failures from login attempts by hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Top Hosts by Number of Connections	This query returns host information and the number of events in which the category behavior is /Access/Start and the category outcome is not Failure.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/
SNMP Authentication Failures by Device	This query returns events with authentication or authorization failures using SNMP. The query returns the device information sorted by count, from highest to lowest.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/Device SNMP Authentication Failures/
Device SNMP Authentication Failures by User	This query returns events with authentication or authorization failures using SNMP. The query returns user information sorted by count, from highest to lowest.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/Device SNMP Authentication Failures/
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/ Cross-Device/
Device SNMP Authentication Failures	This query returns events with authentication or authorization failures using SNMP.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network/Device SNMP Authentication Failures/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
Chart and 2 Tables Landscape	This template is designed to show one chart and two tables. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With 2 Tables
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Two Charts One Table Landscape	This template is designed to show two charts and a table. The orientation is landscape.	Report Template	ArcSight System/2 Charts/With Table
User Sessions	This session list tracks Identity Management user session starts and stops (or terminations). The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, increase the Entry Expiration Time. The sessions are maintained by the User Session (Identity Management) Started and User Session (Identity Management) Stopped rules.	Session List	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/

**Resources that Support the Login Tracking Group, continued**

Resource	Description	Type	URI
User VPN Sessions	This session list tracks VPN user session starts and stops (or terminations), for purposes of tracking user session durations. The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	Session List	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/



## Reconnaissance

The Reconnaissance resources expand on the ArcSight Core reconnaissance rules, and provide insight into the different types of reconnaissance directed at the network or parts of the network. This content breaks down reconnaissance activity by type. Dashboards show what parts of the network are being scanned and how.

The following device types can supply events that apply to the Reconnaissance resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Reconnaissance Resource Group

The Reconnaissance resource group requires the following configuration for your environment.

Enable the following trends:

- **Reconnaissance Activity**—This trend collects a daily snapshot of events using the Reconnaissance Activity Trend query. The Scanning Activity by Business Role Trend report is based on this trend.
- **Reconnaissance Types Detected**—This trend collects a daily snapshot of events. The data is used by the Top 10 Reconnaissance Types Detected trend.
- **Top 10 Reconnaissance Types Detected**—This trend collects the top ten reconnaissance event types per day from the Reconnaissance Types Detected trend. This data is used by the Reconnaissance Types Detected Trend report.

## Reconnaissance Resources

The following table lists all the resources in the Reconnaissance group.

### Resources that Support the Reconnaissance Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Reconnaissance Activity	This active channel shows reconnaissance events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
Reconnaissance in Progress	This dashboard displays the Top 10 Zones Scanned, the Last 10 Zones Scanned, the Last 10 Hosts Scanned, and the Last 10 Scanners data monitors to give an overview of the reconnaissance activity against the network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Graph	This dashboard displays the Reconnaissance Graph data monitor to provide operators and analysts a view into how reconnaissance events are probing the network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/
Port Scanning Activity Trend	This report displays a chart showing the top transport protocol and target port pairs (Protocol - Port) by target zone over the last 7 days based on summary data from the Port Scanning trend. The report also presents a table showing the daily summary of the top 20 prioritized event counts from each zone for the protocol - port pairs from the Port Scanning Daily Top 20 trend.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Scanning Activity by Business Role Trend	This report displays a daily trend of scanning events related to business roles over the past seven days and a table giving a simple breakdown of the activity charted.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Types Detected Trend	This report shows the daily event activity summary for the different reconnaissance types over the past seven days (based on ArcSight System rules with names beginning with Reconnaissance - and differentiated by the type names Distributed Host Port Scan, Distributed Network Host Scan, Multiple Host Scan, Network Service Scan, Script Scan, Stealthy Host Port Scan, and Vulnerability Scan). A table shows the daily breakdown and zone information charted. The Row Limit is set to 70 (top 10 * 7 days). To extend the time frame, change the row limit accordingly. Note: The Top 10 Reconnaissance Types Detected and the Reconnaissance Types Detected trends are disabled by default. This	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
	report does not show any results until these trends have been enabled and have become sufficiently populated.		
Prioritized Scanning Activity by Zone	This report shows the numbers of events, by priority and target zone, over the past hour. A table shows the zones in order of highest event counts by the priority of the events (from highest priority to lowest).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/
Prioritized Scanning Activity by Business Role	This report shows the activity levels and priorities of reconnaissance events directed at assets within the various business role categories.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Scanning Activity by Zone Trend	This report shows the daily trend of the most frequent reconnaissance events and a daily prioritized breakdown of those events by zone over the last seven days. The report uses two separate queries, one for the table and a simpler one for the chart, on the Zone Scanning Events by Priority trend.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Types Detected by Zone	This report presents a chart with the event activity over the past hour of the different reconnaissance types (based on ArcSight System rules with names beginning with Reconnaissance - and differentiated by the type names Distributed Host Port Scan, Distributed Network Host Scan, Multiple Host Scan, Network Service Scan, Script Scan, Stealthy Host Port Scan, and Vulnerability Scan) A table shows the breakdown and zone information charted.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/
Port Scanning Activity	This report presents a chart of the most frequently occurring events for transport protocol/target port pairs by zone. A table shows more data points for additional information beyond that presented in the chart.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/



**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
<b>Library - Correlation Resources</b>			
Firewall - Host Port Scan	This rule looks for port scans on a host. The rule monitors failure access detected by a firewall. The rule triggers when three events occur within three minutes with the same attacker/target pair with different target ports each time. On the first threshold, the attacker address is added to the Reconnaissance active list and the target address is added to the Scanned active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Firewall - Application Protocol Scan	This rule detects application protocol scans. The rule monitors failure access detected by a firewall. The rule triggers when three events occur within three minutes with the same attacker/target pair with different application protocols each time. On the first threshold, the attacker address is added to the Reconnaissance active list and the target address is added to the Scanned active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
Attack from Source having Reconnaissance History	This rule detects attacks from sources that have already performed reconnaissance. This rule triggers when the attacker is in the Reconnaissance or Untrusted active list and the event has hostile or compromise significance. On the first event, the attacker is added to the Hostile active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Firewall - Network Port Scan	This rule looks for a network port scan. The rule monitors failure access detected by a firewall. The rule triggers when five events occur within three minutes with the same port for each attacker/target pair, but with different target addresses each time. On the first threshold, the attacker address is added to the Suspicious active list and the target address is added to the Scanned active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
<b>Library Resources</b>			
Hostile List	This Active List contains hosts that have been attempting attacks on systems.	Active List	ArcSight System/Threat Tracking
Suspicious List	This Active List contains hosts which have performed suspicious activity, either on the local system or over the network.	Active List	ArcSight System/Threat Tracking

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	Active List	ArcSight System/Attackers
Reconnaissance List	This Active List contains IP addresses of hosts which have performed reconnaissance activity.	Active List	ArcSight System/Threat Tracking
Scanned List	This Active List contains hosts that have been scanned by a potential attacker.	Active List	ArcSight System/Targets
Business Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Last 10 Hosts Scanned	This data monitor shows the target zone and address, along with the time, of the last ten reconnaissance events, providing an overview of the most recent scanning activity against specific hosts.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Top 10 Zones Scanned	This data monitor shows the target zone of the ten most frequent reconnaissance events within the last hour, providing an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Last 10 Zones Scanned	This data monitor shows the time and the target zone of the last ten reconnaissance events, providing an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Last 10 Scanners	This data monitor shows the attacker zone and address, along with the time, of the last ten reconnaissance events to give an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Reconnaissance Graph	This data monitor provides operators and analysts a view into how reconnaissance events are probing the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance Graph/
Not Correlated and Not Closed and Not Hidden	This filter selects events that have not had their event annotation flags set to correlated (by a rule), close (by an analyst) or hidden (by system settings).	Filter	ArcSight System/Event Types
Reconnaissance Events by Target	This filter identifies events where the target address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Events by Target Zone	This filter identifies events where the target zone is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Reconnaissance Events by Attacker	This filter identifies events where the attacker address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Events (Internal Targets)	This filter identifies events that match the Internal Target, Not Correlated and Not Closed and Not Hidden, and Non-ArcSight Internal Events filters and one or more conditions where the event name starts with Reconnaissance, the category significance is Recon, or the category technique starts with Scan. This is the foundation filter for the other Reconnaissance filters: Reconnaissance Events by Attacker, Reconnaissance Events by Target, and Reconnaissance Events by Target Zone.	Filter	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types



**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Zone Scanning Events	This query returns the target zone resource, the priority, and sums the aggregated event count of events for the chart and table in the Prioritized Scanning Activity by Zone report. The events are selected by the Reconnaissance Events by Target Zone filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/
Top 10 Reconnaissance Types Detected on Trend	This query returns the top ten reconnaissance event types per day from the Reconnaissance Types Detected trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Types Detected on Trend	This query returns the date, the target zone, the event name and the sum of the aggregated event count from the summary of the Top 10 Reconnaissance Types Detected trend for the Daily Breakdown of Reconnaissance Types Detected table in the Reconnaissance Types Detected Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Reconnaissance Types Detected	This query returns the target zone resource, reconnaissance type (event name), and sums the aggregated event count of events where the event name starts with Reconnaissance but not Reconnaissance - In Progress, matches the Reconnaissance Events (Internal Target) filter, and is a correlation event (event type = 2), for the Reconnaissance Types Detected by Zone report.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Ports Scanned	This query returns the target zone resource, the transport protocol and target port pair as a variable (dvProtocol-Port), and sums the aggregated event count of events where the target port is provided and matching the Reconnaissance Events (Internal Target) filter for the table and chart in the Port Scanning Activity report.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/
Business Roles Scanned	This query returns the business role via a variable (dvBusinessRole), the priority, and sums the aggregated event count of events matching the Reconnaissance Events (Internal Target) filter targeting assets categorized by the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/ category.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Port Scanning Daily Top 20, Trend on Trend	This query returns the target zone resource, priority, transport protocol, target port, and sums the aggregated event count for the summary data from the Port Scanning trend to populate the Port Scanning Daily Top 20 trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/Trend Queries/
Port Scanning Trend	This query returns the target zone resource, transport protocol, target port, priority, and sums the aggregated event count of events where the target port is provided and match the Reconnaissance Events (Internal Target) filter to populate the Port Scanning trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/Trend Queries/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Zone Scanning Events by Priority Trend	This query returns the target zone resource, the priority, and sums the aggregated event counts of events selected by the Reconnaissance Events by Target Zone filter for the Zone Scanning Events by Priority trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/Trend Queries/
Daily Port Scanning Activity on Trend	This query returns the date via a variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning Daily Top 20 trend for the Daily Top 20 Protocol and Ports by Zone table in the Port Scanning Activity Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Types Detected on Trend (Chart Query)	This query returns the date, the reconnaissance type (event name), and a sum of the aggregated event count from summary information in the Top 10 Reconnaissance Types Detected trend. This query provides data for the Daily Reconnaissance Types Detected chart in the Reconnaissance Types Detected Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Daily Port Scanning Activity on Trend (Chart Query)	This query returns the date via a variable (dvDate), the target zone resource, the priority, the transport protocol, the target port, and sums the aggregated event count from the summary provided by the Port Scanning trend for the Top 20 Protocol and Ports by Count from MM-DD-YYYY to MM-DD-YYY-HH:MM:SS chart in the Port Scanning Activity Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Activity Trend	This query returns the target zone resource, the attacker zone resource, the category significance, category technique and sums the aggregated event count of events using the Reconnaissance Events by Target filter for the Reconnaissance Activity trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/Trend Queries/
Reconnaissance Types Detected Trend	This query returns the target zone resource, event name, priority and sums the aggregated event count of event data for the Reconnaissance Types Detected trend. The events are filtered by the Reconnaissance Events (Internal Targets) filter, the event name starting with Reconnaissance but not the Reconnaissance - In Progress event.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/Trend Queries/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Zone Scanning Activity on Trend	This query returns the date, the priority, the target zone resource, and sums the aggregated event count from the Zone Scanning Events by Priority trend for the Daily Breakdown of Zone Scanning Activity by Priority table in the Scanning Activity by Zone Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Daily Scanning Events by Business Role on Trend	This query returns the date, the business role via a variable (dvBusinessRole), and sums the aggregated event count of the data from the Reconnaissance Activity trend. This query provides both chart and table data for the Scanning Activity by Business Role Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/



**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Zone Scanning Activity on Trend (Chart Query)	This query returns the date, the target zone resource, and sums the aggregated event counts from the Zone Scanning Events by Priority trend to provide data for the Daily Zone Scanning Activity chart in the Scanning Activity by Zone Trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Port Scanning Daily Top 20	This trend provides a daily snapshot of the top events in the Port Scanning trend. Up to 20 events per day are collected for use as detailed daily information in the Port Scanning Activity trend. The Port Scanning trend collects the top events for the day and this trend follows up and collects summary information.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Types Detected	This trend collects a daily snapshot of events using the Reconnaissance Types Detected Trend query. Up to 1000 events per day are collected to collect the most common reconnaissance types This data is used by the Top 10 Reconnaissance Types Detected trend. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Port Scanning	This trend collects a daily snapshot of the top 1000 events in for use as detailed daily information in the Port Scanning Activity Trend report. The Port Scanning trend collects the top events for the day and the Port Scanning Daily Top 20 trend (a trend on this trend), follows up and collects summary information.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Zone Scanning Events by Priority	This trend collects a daily snapshot of events using the Zone Scanning Events by Priority Trend query. Up to 1000 events per day are collected. The data is used by the Scanning Activity by Zone Trend report.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
Top 10 Reconnaissance Types Detected	This trend returns the top ten reconnaissance event types per day from the Reconnaissance Types Detected trend. This data is used by the Reconnaissance Types Detected Trend report. Note: This trend is not enabled by default. It also depends on the Reconnaissance Types Detected trend, which is also not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

**Resources that Support the Reconnaissance Group, continued**

Resource	Description	Type	URI
Reconnaissance Activity	This trend collects a daily snapshot of events using the Reconnaissance Activity Trend query. Up to 1000 events per day to collect data for the Scanning Activity by Business Role trend. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/

## Regulated Systems

The Regulated Systems resources focus on events related to assets that have been categorized as one of the compliance requirement asset categories, such as HIPAA, Sarbanes-Oxley, and FIPS-199.

The following device types can supply events that apply to the Regulated Systems resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Regulated Systems Resource Group

Categorize all regulated systems in your environment with the **Compliance Requirement** or the **Sarbanes-Oxley** asset category. For more information about categorizing assets, refer to ["Categorizing Assets" on page 11](#).

## Regulated Systems Resources

The following table lists all the resources in the Regulated Systems group.

### Resources that Support the Regulated Systems Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Regulated Systems - By Host - Attacked	This report shows the target host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category, that match the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/
Regulated Systems - Count Vulnerabilities	This report shows the compliance requirement, asset name, and the count of vulnerabilities for assets in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/

**Resources that Support the Regulated Systems Group, continued**

Resource	Description	Type	URI
Regulated Systems - By Attack	This report displays the event name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category, that match the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/
Sarbanes-Oxley - Top 10 Targets	This report displays the target host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/Reporting Requirement/Sarbanes-Oxley asset category, that match the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Regulated Systems/
<b>Library Resources</b>			
Compliance Requirement	This is a site asset category.	Asset Category	Site Asset Categories
Sarbanes-Oxley	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Data Role/Reporting Requirement
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Regulated Systems - By Attack	This query returns the event name and the sum of the aggregated event count for events with Target Asset IDs in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category, that match the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/

**Resources that Support the Regulated Systems Group, continued**

Resource	Description	Type	URI
Sarbanes-Oxley - Top 10 Targets	This query returns the target Host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/Reporting Requirement/Sarbanes-Oxley asset category, that match the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Regulated Systems/
Regulated Systems - By Host - Attacked	This query returns the target host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category, that match the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/
Regulated Systems - Count Vulnerabilities	This query returns the compliance requirement, asset name, and the count of vulnerabilities for assets in the /All Asset Categories/Site Asset Categories/Compliance Requirement asset category.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Regulated Systems/
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## Resource Access

The Resource Access resources focus on access events, broken down by resource types, such as (database, email, files, and so on) and track this access by user. The brute force resource activity is included here. There are session lists that track the duration of an access session by user, and the duration of access sessions that took place after a brute force login attack.

The following device types can supply events that apply to the Resource Access resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Resource Access Resource Group

The Resource Access resource group requires the following configuration for your environment.

Enable the following trends:

- **Daily Top 10 Resource Access Trends**—You can use this trend to generate a report.
- **Resource Access**—The data from this trend is used by the Daily Top 10 Resource Access Trends trend.



## Resource Access Resources

The following table lists all the resources in the Resource Access group.

### Resources that Support the Resource Access Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Access Initiation Events	This active channel shows events received during the last two hours and includes a sliding window that displays the last two hours of event data. A selection of three filters restricts the events shown in the active channel only to those related to access initiation, authentication verification, or authorization verification for database, email, and file resources.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Resource Access/
All Access and Authentication Events	This active channel shows events received during the last two hours and includes a sliding window that displays the last two hours of event data. A selection of three filters restricts the events shown in the active channel only to those related to access and authorization for any resource.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Access Termination Events	This active channel shows events received during the last two hours and includes a sliding window that displays the last two hours of event data. A selection of three filters restricts the events shown in the active channel only to those related to access termination for database, email, and file resources.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Resource Access/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Resource Access Trend	This report displays unusual resource access attempt trends for each of the past seven days. The range of outcomes is failure, attempt or success. An outcome of attempt means that there is not sufficient information to determine if the attempt succeeded. Note: An outcome of success means that there is enough information to know that the resource was accessed, but the access initiation does not fit in the normal access initiation pattern. The Resource Access trend is disabled by default.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Brute Force Session Trends	This report shows trend information about active and closed resource access sessions after a successful brute force attack. The data for this report comes from the Brute Force Resource Access (keyed by target) session list.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Access Events by Database Resource	This report displays unusual database resource access attempts. The range of outcomes is failure, success, or attempt (there is not sufficient information to determine if the attempt succeeded). Note: An outcome of success means that there is enough information to know that the database resource was accessed, but the access initiation does not fit in the normal database access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Brute Force Access Activity	This report displays information about active and closed resource access sessions after a successful brute force attack. The data for this report comes from the Brute Force Resource Access (keyed by target) session list.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Access Activity	This report gives the details of active and closed resource access sessions based on session information in the Resource Access session list. The Resource Access session list contains an entry expiration of four days, so the report parameters are set to cover all the entries, up to the row limits set in the parameters.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/
Email Resource Access by Users	This report displays successful and unusual email resource access attempt information. The range of outcomes is failure, attempt or success. An outcome of attempt means that there is not sufficient information to determine if the attempt succeeded. Note: An outcome of success means that there is enough information to know that the resource was accessed, but the access initiation did not fit in the normal access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Database Resource Access by Users	This report displays successful database access and failed or attempted database access events. The range of outcomes is failure, success, or attempt (there is not sufficient information to determine if the attempt succeeded. Note: An outcome of success means that there is enough information to know that the resource was accessed, but the access initiation did not fit in the normal access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Access Events by File Resource	This report displays unusual file access attempts. The range of outcomes is failure, attempt or success. An outcome of attempt means that there is not sufficient information to determine if the file access attempt succeeded. Note: An outcome of success means that there is enough information to know that the file was accessed, but the access did not fit in the normal pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
File Resource Access by Users	This report displays successful file access, and failed or attempted file access events. The range of outcomes is failure, success, or attempt. An outcome of attempt means that there is not sufficient information to determine if the attempt succeeded. An outcome of success means that there is enough information to know that the resource was accessed, but the access initiation does not fit in the normal access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Resource Access by Users	This report displays successful access, and failed or attempted access events. The range of outcomes is failure, success, or attempt. An outcome of attempt means that there is not sufficient information to determine if the attempt succeeded. An outcome of success means that there is enough information to know that the resource is accessed, but the access initiation does not fit in the normal access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Access Events by Email Resource	This report displays unusual email resource access attempts. The range of outcomes is failure, success, or attempt (there is not sufficient information to determine if the attempt succeeded). Note: An outcome of success means that there is enough information to know that the email resource was accessed, but the access initiation does not fit in the normal email access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Access Events by Resource	This report displays unusual resource access attempts. The range of outcomes is failure, success, or attempt (there is not sufficient information to determine if the attempt succeeded). Note: An outcome of success means that there is enough information to know that the resource was accessed, but the access initiation does not fit in the normal access initiation pattern.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Daily Top 10 Resource Access Trends	This report displays unusual resource access attempt trends for the past seven days. The range of outcomes is failure, success, or attempt (there is not sufficient information to determine if the attempt succeeded). Note: Success means that there is enough information to know that the resource was accessed, but the access initiation does not fit in the normal access initiation pattern. The data for this report is collected from a trend on a trend. The first trend collects the raw trend data, at least two magnitudes more than the top 10, and the second trend picks out the top ten for each day. The row limit is set to 70, which gives the top 10 events for the past seven days. To see the past ten days, set the row limit to 100. Note: The Daily Top 10 Resource Access Trends is disabled by default. When you enable this trend, make sure you also enable the Resource Access base trend.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
<b>Library - Correlation Resources</b>			
Resource Access Initiation	This rule detects resource access initiation events as defined by the Access Initiation Events filter and adds an entry in the Resource Access session list	Rule	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Resource Access Termination	This rule detects resource access termination events as defined by the Access Termination Events filter, and terminates the sessions in the Brute Force Resource Access and Resource Access session lists.	Rule	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Brute Force Resource Access Initiation	This rule detects brute force resource access initiation events (defined by the Access Initiation Events filter) and adds an entry in the Brute Force Resource Access session list.	Rule	ArcSight Foundation/Intrusion Monitoring/Resource Access/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
<b>Library Resources</b>			
Worm Infected Systems	This active list is automatically populated by rules that have detected worm activity on a given system.	Active List	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Resource Access	<p>This field set shows the fields of interest when monitoring resource access events and includes the following fields: End Time Name Resource Type * User ID * User Name * Resource Zone Name * Resource Address * Device Vendor Device Product Access Outcome * Priority Agent Name Attacker Zone Name Attacker Address</p> <p>* These fields are aliased by means of variables, where: Resource Type = Category Object User ID = Target User ID User Name = Target User Name Resource Zone Name = Target Zone Name Resource Address = Target Address Access Outcome = Category Outcome</p>	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Access to Database Resources	This filter returns events in which the category object is /Host/Application/Database. The filter is designed to focus on specific events identified by the Access Initiation Events filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Access to Email Resources	This filter identifies events in which the category object is /Host/Application/Service/Email.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Access to File Resources	This filter identifies events in which the category object is /Host/Resource/File.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Access Termination Events	This filter identifies events in which the category behavior is /Access/Stop and the event also matches the Access to Database Resources, Access to Email Resources, or Access to File Resources filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/
All Access and Authentication Events	This filter identifies events in which the category behavior is Access, Authentication, or Authorization.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Access Initiation Events	This filter identifies events in which the category behavior is /Access/Start, /Authentication/Verify, /Authorization/Verify, and the event also matches the Access to Database Resources, Access to Email Resources, or Access to File Resources filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Daily Top 10 Resource Access on Trend	This query returns data from the Daily Top 10 Resource Access Trends query for use in the Daily Top 10 Resource Access Trends report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Daily Top 10 Resource Access on Trend	This query returns data from the Resource Access trend for input into the Daily Top 10 Resource Access trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/Trend Queries/



**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Resource Accesses	This query returns data for the Resource Access Events by Users reports. The data selected is related to the resource type, the resource zone and address, the outcome of the event (successful), the user name and ID, and the number of times the event has been recorded for that resource by that user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Brute Force Access Closed Sessions on Trend	This query returns closed session trend information from the Brute Force Access Session Trends trend for the Brute Force Session Trends report. A closed session is one with a start and end time, and the query provides a field (Dependent Variable) that gives the difference in these times, (the duration of the session).	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Access Active Sessions	This query returns data from the Resource Access (keyed by target) session list. The data selected is resource, user and attacker information for sessions that have not been reported closed, and are assumed to still be active.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/
Access Closed Sessions	This query returns data from the Resource Access (keyed by target) session list. The data selected is resource, user and attacker information, and length of time the resource was accessed, for sessions that have been reported closed.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/
Brute Force Access Active Sessions on Trend	This query returns open session trend information from the Brute Force Access Session Trends trend for the Brute Force Session Trends report. An open session is one with a start time, but no end time.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Resource Access on Trend	This query returns the date, resource type, outcome, user ID, user name, resource zone, resource address and the count of events for these events from the Resource Access trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Brute Force Access Sessions Trend	This query returns data from the Brute Force Resource Access session list to collect data for the Brute Force Access Sessions trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/Trend Queries/
Resource Access Attempts	This query returns data for the Resource Access Events by Users reports. The data selected is related to the resource type, the resource zone and address, the outcome of the event (attempt or fail), the user name and ID, and the number of times the access initiation attempt has been recorded for that resource by that user.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Brute Force Access Active Sessions	This query returns data from the Brute Force Resource Access (keyed by target) session list. The data selected is resource, user and attacker information for sessions that have not been reported closed, and are assumed to still be active.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/
Brute Force Access Closed Sessions	This query returns data from the Brute Force Resource Access (keyed by target) session list. The data selected is resource, user and attacker information, and length of time the resource was accessed, for sessions that have been reported closed.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Sessions/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Resource Access Trend	This query returns event data for the Resource Access trend. The event data fields collected are:  Category Object  Category Outcome  Target User ID  Target User Name  Target Zone Resource  Target Address  and the count of the number of times the events occurred for that resource.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/Trend Queries/
Access Attempts by Resource	This query returns data for the Access Events by Resource reports. The data selected is related to the resource type, the resource zone and address, the outcome of the event, and the number of times the event has been recorded for that resource.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Resource Access/Reports on Access Events/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Two Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/2 Tables
Two Tables Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/2 Tables
Brute Force Resource Access	This session list stores information about resource access after a detected brute force attack, including the initial time and duration of the access. If the end time is blank, the session is open. The session automatically closes after four days because the resource might not report the session termination.	Session List	ArcSight Foundation/Intrusion Monitoring/Resource Access/

**Resources that Support the Resource Access Group, continued**

Resource	Description	Type	URI
Resource Access	This session list stores information about abnormal resource access, including the initial time and duration of the access. If the end time is blank, the session is open. The session automatically closes after four days because the resource might not report the session termination.	Session List	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Daily Top 10 Resource Access Trends	This trend tracks the top ten resource access attempts stored in the Resource Access Trends trend. The trend runs once per day, checks all of the events from the Resource Access Trends trend, and selects the top ten entries by count. Note: This trend is disabled by default. To work properly, this trend and its base trend, Resource Access, need to be enabled.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Brute Force Access Session Trends	This trend tracks resource access sessions following brute force attacks.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/
Resource Access	This trend tracks unusual resource access attempts, including the outcome of the access attempt. Note: This trend is not enabled by default. When enabled, this trend runs daily, covering a full day.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Resource Access/

## Revenue Generating Systems

The Revenue Generating Systems resources provide reports that focus on attacked or compromised systems that have been categorized in the Revenue Generation category under Business Impact Analysis/Business Roles.

The following device types can supply events that apply to the Revenue Generating Systems resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Revenue Generating Systems Resources

The following table lists all the resources in the Revenue Generating Systems group.

### Resources that Support the Revenue Generating Systems Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Revenue Generating Systems - Attacked	This report displays the target host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - All	This report displays the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category outcome of success.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/

**Resources that Support the Revenue Generating Systems Group, continued**

Resource	Description	Type	URI
Revenue Generating Systems - Compromise - Confidentiality	This report displays the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category technique of Information Leak and a category outcome of success.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - Availability	This report displays the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category technique of DoS and a category outcome of success.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - Integrity	This report displays the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category technique that is not DoS or starts with Information Leak, and a category outcome of success.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
<b>Library Resources</b>			
Revenue Generation	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
All Events	This filter matches all events.	Filter	ArcSight System/Core

**Resources that Support the Revenue Generating Systems Group, continued**

Resource	Description	Type	URI
Revenue Generating Systems - Compromise - Confidentiality	This query returns the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category technique of Information Leak and a category outcome of success.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - Availability	This query returns the target host name and the count of vulnerabilities for events with Target Asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a Category Technique of DoS and a Category Outcome of success.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - Integrity	This query returns the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a category technique that is not DoS or starts with Information Leak, and a category outcome of success.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Revenue Generating Systems - Compromise - All	This query returns the target host name and the count of vulnerabilities for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter with a Category Outcome of success.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/

**Resources that Support the Revenue Generating Systems Group, continued**

Resource	Description	Type	URI
Revenue Generating Systems - Attacked	This query returns the target host name and the sum of the aggregated event count for events with target asset IDs in the /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset category, matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Revenue Generating Systems/
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table



## SANS Top 5 Reports

The SANS Top 5 Reports resources provide information that helps address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports.

The following device types can supply events that apply to the SANS Top 5 Reports resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems
- Vulnerability scanners

## SANS Top 5 Reports Resources

The following table lists all the resources in the SANS Top 5 Reports group.

### Resources that Support the SANS Top 5 Reports Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Protocol Distribution Report	This report shows the top busiest protocols.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Traffic by Transport Protocol	This report shows the traffic repartition by transport protocol by minute for the last hour.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Traffic Moving Average Report	This report shows the moving average of ICMP, UDP, and TCP Traffic for the last hour.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 10 Talkers	This report shows the top ten talkers.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/

### Resources that Support the SANS Top 5 Reports Group, continued

Resource	Description	Type	URI
Top List of Accessed Web Sites	This report shows the top accessed web sites.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top Target IPs	This report shows the top target IP addresses.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top Source Ports	This report shows the busiest source ports.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 10 Types of Traffic	This report shows the top ten types of traffic.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top List of Highest Bandwidth-Consuming Conversations	This report shows the highest bandwidth-consuming conversations.	Report	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
<b>Library Resources</b>			
TCP Traffic	This filter identifies TCP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
UDP Traffic	This filter identifies UDP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/
ICMP Traffic	This filter is used to identify ICMP Traffic.	Filter	ArcSight Foundation/Network Monitoring/Report Parameter Filters/

**Resources that Support the SANS Top 5 Reports Group, continued**

Resource	Description	Type	URI
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Foundation/Network Monitoring/Connector Filters/
Top Targets	This query retrieves the target ports with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top Target IPs/
Top Source Ports	This query retrieves the attacker ports with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top Source Ports/
Traffic by Transport Protocol	This query retrieves the number of total bytes (Bytes In + Bytes Out) by transport protocol within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Traffic by Transport Protocol/
Top Protocols	This query retrieves the protocol with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 10 Types of Traffic
Top Attacker-Target Pairs	This query retrieves the attacker-target pairs with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top List of Highest Bandwidth-Consuming Conversations/
Top Accessed Web Sites	This query retrieves the target address or zone of the websites with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top List of Accessed Web Sites/

**Resources that Support the SANS Top 5 Reports Group, continued**

Resource	Description	Type	URI
Top Attackers	This query retrieves the attacker or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 10 Talkers/
Traffic Spike Rule Fired Events	This query retrieves correlation events generated by moving average data monitors looking for TCP, UDP, and ICMP spikes within the last hour.	Query	ArcSight Foundation/Network Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Traffic Moving Average Report/
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table
Three Tables Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/3 Tables
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## SANS Top 20

The SANS Top 20 resources provide the context for a series of email and operating system rules that look for specific events that relate to vulnerabilities. The SANS Top 20 reports show assets where these vulnerabilities have been compromised.

The following device types can supply events that apply to the Sans Top 20 resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems
- Vulnerability scanners

## Configuring the SANS Top 20 Resource Group

Enable the **SANS Top 20 (v6.01) Attacked Systems** trend. The data from this trend is used for the Trend: Inbound DoS Events - Yesterday, the SANS Top 20 (v6.01) Vulnerability Area Activity - Hourly Report and the SANS Top 20 (v6.01) Attacked Systems - Hourly Report.

## SANS Top 20 Resources

The following table lists all the resources in the SANS Top 20 group.

### Resources that Support the SANS Top 20 Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Trend: Inbound DoS Events - Yesterday	This report displays the target zones and the associated number of DoS events per hour.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 (v6.01) Vulnerability Area Activity - Hourly Report	This report shows the different SANS Top 20 Vulnerability areas (Operating System, Email, and so on) and how many attacks for each area have occurred in the last 60 minutes. This report uses data generated by events from the SANS Top 20 rules.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/SANS Top 20/
SANS Top 20 (v6.01) Attacked Systems - Hourly Report	This report provides a view of the different SANS Top 20 Vulnerabilities and how many attacks for each vulnerability have occurred within the last 60 minutes. The report uses data generated by events from the SANS Top 20 rules.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/SANS Top 20/
<b>Library - Correlation Resources</b>			

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft Task Scheduler Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft Task Scheduler vulnerability. The Microsoft Windows Task Scheduler is an ActiveX control that schedules arbitrary commands to be run on a system. There is a buffer overflow in the scheduler due to not properly checking attributes of the command names tasked within the scheduler. The rule checks for events related to inbound traffic categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB:MS04-022 or CVE:CAN-2004-0212. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken: An event is sent with the following additional settings: name: SANS Top 20 (v6.01) - Microsoft Task Scheduler Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft Task Scheduler Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-022 and CVE:CAN- 2004-0212.</p>		



#### Resources that Support the SANS Top 20 Group, continued

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft WINS Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for WINS vulnerabilities. The Windows Internet naming Service (WINS) provides a mapping between NETBIOS computer names and IP addresses. Incoming WINS packets are not sufficiently validated on the name parameter, allowing a buffer overflow. Additionally, there is a heap-based buffer overflow in the server-to-server replication protocol due to not properly validating the association context data structure. The rule checks for events related to inbound traffic on port 42 (UDP or TCP), categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB:MS04-045, CVE:CAN-2004-0567 or CVE:CAN-2004-1080. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft WINS Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft WINS Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-045, CVE:CAN-2004-0567 and CVE:CAN-2004-1080</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft SMB Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft SMB Service vulnerability. The Microsoft Server Message Block (SMB) protocol allows sharing of files, printers, serial ports, and so on. There are flaws in SMB packet validation that might result in a buffer receiving inappropriate data. The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB:MS05-011 or MSSB:MS05-027. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft SMB Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft SMB Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-011, MSSB:MS05-027, CVE:CAN-2005-0045 and CVE:CAN-2005-1206.</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 Email (v6.01) - Microsoft Office XP Buffer Overflow Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W4 Microsoft Office and Outlook Express for the Microsoft OLE and COM Remote Code Execution vulnerabilities (see <a href="http://www.sans.org/top20/2005/#w4">http://www.sans.org/top20/2005/#w4</a> for details).</p> <p>There is a buffer overflow error in Microsoft Office XP that might allow an attacker to gain full control of a system where the user is tricked into clicking on a link to a malicious file, either from an email message or through Internet Explorer.</p> <p>The rule checks for base events related to outbound traffic from an application with behavior categorized as Communicate/Query or starting with Access, with an outcome of no failure, from source systems with a Microsoft operating system.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name = SANS Top 20 Email (v6.01) - Microsoft Office XP buffer overflow vulnerability Exploit Attempt</p> <p>agentSeverity = Medium</p> <p>categoryBehavior = /Communicate/Query</p> <p>categoryObject = /Host/Operating System, categoryOutcome = /Attempt</p> <p>categorySignificance = /Compromise</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Email/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categoryTechnique = /Exploit/Vulnerability</p> <p>deviceCustomString1Label = Rule Type</p> <p>deviceCustomString1 = SANS Top 20 (v6.01)</p> <p>deviceCustomString2Label = Vulnerability Area</p> <p>deviceCustomString2 = Email</p> <p>deviceCustomString3Label = Vulnerability Name</p> <p>deviceCustomString3 = Microsoft Office XP buffer overflow vulnerability Exploit Attempt</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-005 and CVE:CAN-2004-0848.</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft Plug and Play Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft Plug and Play Service vulnerability.</p> <p>The Microsoft Plug and Play Service contains buffer overflows that can allow a remote user to execute arbitrary code.</p> <p>The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB MS05-039 or MSSB MS05-047. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft Plug and Play Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft Plug and Play Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB MS05-039, MSSB MS05-047, CVE CAN-2005-1983 and CVE CAN-2005-2120.</p> <p>"</p>		



**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft NetDDE Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft NetDDE Service vulnerability.</p> <p>The Microsoft Network Dynamic Data Exchange (NetDDE) protocol has a buffer management flaw in the way malformed messages are handled that exposes a vulnerability that might allow an attacker to compromise the vulnerable system.</p> <p>The rule checks for events related to inbound traffic on TCP ports 135, 139, 445 or 593, or UDP port 135, 137, 138 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft NetDDE Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft NetDDE Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-031 and CVE:CAN- 2004-0206.</p>		

#### Resources that Support the SANS Top 20 Group, continued

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft NNTP Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft NNTP Service vulnerability. The Microsoft Network News Transport Protocol (NNTP) Service in Internet Information Services (IIS) has several flaws in the way the NNTP component handles the parsing of user search patterns for the XPAT command. A remote, unauthenticated attacker might execute arbitrary code with administrative privileges on a vulnerable system. The rule checks for events related to inbound traffic on ports 119 or 563 (TCP or UDP), categorized as hostile or compromise, with an outcome of no failure, to assets with the vulnerability category MSSB:MS04-036 or CVE:CAN-2004-0574. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft NNTP Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft NNTP Service Vulnerabilities</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-036 and CVE:CAN-2004-0574.</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft License Logging Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft License Logging Service vulnerabilities.</p> <p>The Microsoft License Logging service has an unchecked buffer that might allow an attacker to remotely execute arbitrary code.</p> <p>The rule checks for events related to inbound traffic on TCP ports 139 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft License Logging Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.01)</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft License Logging Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-010 and CVE:CAN- 2005-0050.</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft Exchange SMTP Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a> for details) for the Exchange SMTP Service vulnerability.</p> <p>There is a buffer overflow error in the way that Exchange (2000 and Server 2003) handles an SMTP extension that might allow a remote attacker to execute arbitrary code or cause a denial of service.</p> <p>The rule checks for events related to inbound traffic categorized as hostile or compromise, with an outcome of no failure, to target systems with a Microsoft operating system on port 25.</p> <p>It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group. If the target system is not in the Microsoft operating system Asset Group, the asset ID should either be NULL or not in any Operating System group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft Exchange SMTP Service Vulnerability Exploited</p> <p>agentSeverity: Very High</p> <p>categoryBehavior: /Communicate/Query</p> <p>categoryObject: /Host/Operating System</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.0.1)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft Exchange SMTP Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-021 and CVE:CAN-2005-0560.</p>		



**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft MSDTC and COM Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft MSDTC and COM+ Services vulnerabilities.</p> <p>The Microsoft Distributed Transaction Coordinator (MSDTC), COM+, Transaction Internet Protocol (TIP) and Distributed TIP services have flaws that might allow an attacker to execute arbitrary code, elevate local privileges or cause a denial of service.</p> <p>The rule checks for events related to inbound traffic on TCP ports 135, 139, 445, 593, 1025 or 3372, or UDP ports 135, 137, 138 or 445, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system's asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft MSDTC or COM+ Services Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p> <p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft MSDTC or COM+ Services Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name</p> <p>The relevant Microsoft Security Bulletins and CE identifiers are MSSB:MS05-051, CVE:CAN- 2005-1978, CVE:CAN-2005- 1979, CVE:CAN-2005-1980 and CVE:CAN-2005-2119.</p>		

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 OS (v6.01) - Microsoft Message Queuing Service Vulnerabilities	<p>This rule checks for the SANS Top 20 vulnerabilities in W1 Windows Services (see <a href="http://www.sans.org/top20/2005/#w1">http://www.sans.org/top20/2005/#w1</a>) for the Microsoft Message Queuing Service vulnerabilities.</p> <p>The Microsoft Message Queuing service has an unchecked buffer that might allow an attacker to remotely execute arbitrary code.</p> <p>The rule checks for events related to inbound traffic on TCP ports 135, 139, 445, 593, 1801, 2101, 2103, 2105 or 2107, or UDP ports 135, 137, 138, 445, 1801 or 3527, categorized as hostile or compromise, with an outcome of no failure. It then looks for events related to traffic from the target system to the attacking system, if the target system asset ID is within the Microsoft operating system Asset Group.</p> <p>If the above conditions are met, the following actions are taken:</p> <p>An event is sent with the following additional settings:</p> <p>name: SANS Top 20 (v6.01) - Microsoft Message Queuing Service Vulnerability Exploited</p> <p>agentSeverity: Very-High</p> <p>categoryBehavior: /Execute</p> <p>categoryObject: /Host/Operating System</p> <p>categoryOutcome: /Success</p> <p>categorySignificance: /Compromise</p> <p>categoryTechnique: /Exploit/Vulnerability</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
	<p>Device Custom String1: SANS Top 20 (v6.01)</p> <p>Device Custom String1 Label: Rule Type</p> <p>Device Custom String2: OS</p> <p>Device Custom String2 Label: Vulnerability Area</p> <p>Device Custom String3: Microsoft Message Queuing Service Vulnerability Exploited</p> <p>Device Custom String3 Label: Vulnerability Name.</p> <p>The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-017 and CVE:CAN-2005-0059.</p>		
SANS Top 20 Email (v6.01) - Microsoft OLE and COM Remote Code Execution Vulnerabilities	This rule checks for the SANS Top 20 vulnerabilities in W4 Microsoft Office and Outlook Express for the Microsoft OLE and COM Remote Code Execution vulnerabilities. There is a buffer overflow error in the way that Exchange (2000 and Server 2003) handles an SMTP extension that could allow a remote attacker to execute arbitrary code or cause a denial of service:MS05-012, CVE:CAN-2005-0044 and CVE:CAN-2005-0047.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Email/
<b>Library Resources</b>			
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Exchange	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type/E mail
Vulnerabilities	This is a site asset category.	Asset Category	Site Asset Categories/Scanned
Microsoft	This is a site asset category.	Asset Category	Site Asset Categories/Operating System
Operating System	This is a site asset category.	Asset Category	Site Asset Categories
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Target Port is not NULL	This filter identifies if an event has an entry for the Target Port field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Successful Inbound DoS Events - Trend Filter	This filter identifies events that are related to successful Denial of Service attacks on internal targets, with the exception of trusted attackers (approved internal vulnerability scanners). This filter is used to select events by a query for a trend on Denial of Service attacks affecting the network, but can also be used for filtering events for a standard event report (not a trend report).	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
Target Asset has Asset Name	This filter is used by some of the query variables to determine if an event has an entry for the Target Asset Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Asset
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol
Successful Inbound DoS Events Query on Trend	This query on the Inbound DoS Events trend returns the target zone name, the target asset name (or its IP address), the service name (Application Protocol Name/Transport Protocol Name: Target Port), a timestamp and sums the number of Denial so Service events against the services on that asset during the time-period (hourly), for the Trend: Inbound DoS Events - Yesterday report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
SANS Top 20 (v6.01) Attacked Systems - hourly	This query collects information about the SANS Top 20 vulnerability areas, vulnerability names, and the number of attacks for each vulnerability on an hourly basis. The data used is generated by events from the SANS Top 20 rules.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/SANS Top 20/
Successful Inbound DoS Events - Trend	This query returns data for reporting the target zone name, the asset name (or IP address), the service name and a summary of event counts. This data is used to populate the Inbound DoS Events trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/Trend Queries/
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Inbound DoS Events	This trend contains data selected by the Successful Inbound DoS Events - Trend query, which selects the day, the service (a variable based on the service name or application protocol, the transport protocol, and the port such as HTML/TCP:80), the TargetAssetName (a variable using the host name, if available, or the IP address), and sums the aggregated event count. Note: This trend is not enabled by default.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Attack Monitoring/DoS/
CVE - CAN-2005-2119	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2005-1206	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2005-0047	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2005-0044	This resource has no description.	Vulnerability	CVE/

**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
MSSB - MS04-045	This resource has no description.	Vulnerability	MSSB/
MSSB - MS05-012	This resource has no description.	Vulnerability	MSSB/
MSSB - MS05-017	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2004-0212	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-011	This resource has no description.	Vulnerability	MSSB/
MSSB - MS05-027	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-0045	This resource has no description.	Vulnerability	CVE/
MSSB - MS04-036	This resource has no description.	Vulnerability	MSSB/
MSSB - MS04-022	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-0050	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-005	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-0059	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-039	This resource has no description.	Vulnerability	MSSB/
MSSB - MS05-010	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-0560	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-021	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-1979	This resource has no description.	Vulnerability	CVE/



**Resources that Support the SANS Top 20 Group, continued**

Resource	Description	Type	URI
CVE - CAN-2005-1980	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2004-0848	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2004-0567	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2004-1080	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2005-1983	This resource has no description.	Vulnerability	CVE/
CVE - CAN-2004-0206	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-051	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2004-0574	This resource has no description.	Vulnerability	CVE/
MSSB - MS04-031	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-1978	This resource has no description.	Vulnerability	CVE/
MSSB - MS05-047	This resource has no description.	Vulnerability	MSSB/
CVE - CAN-2005-2120	This resource has no description.	Vulnerability	CVE/

## Security Overview

The Security Overview resources provide information of interest to executive level personnel.

The following device types can supply events that apply to the Security Overview resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Configuring the Security Overview Resource Group

Categorize all assets that have a business role in your environment with the **Business Role** asset category. For more information about categorizing assets, refer to ["Categorizing Assets" on page 11](#).

## Security Overview Resources

The following table lists all the resources in the Security Overview group.

### Resources that Support the Security Overview Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Intrusion Monitoring - Significant Events	"Overview of hostile, compromise or high priority events. Continuously monitors events matching:  - Not ArcSight Internal Events  - Priority > 8 or Category Significance Starts With /Compromise or /Hostile  Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority)."	Active Channel	ArcSight Foundation/Intrusion Monitoring/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Business Roles	<p>This dashboard displays the status of systems by their business roles: Security Device, Revenue Generation, Infrastructure, Development &amp; Operations and Service. More detailed information is available from the follow-on dashboards in the Detail/Targets groups:</p> <p>Development Assets</p> <p>Infrastructure Assets</p> <p>Operations Assets</p> <p>Revenue Generation Assets</p> <p>Security Device Assets</p> <p>Service Assets</p> <p>This dashboard uses the following data monitors:</p> <p>Status by Security Device Role</p> <p>Status by Infrastructure Role</p> <p>Status by Development and Operations Role</p> <p>Status by Revenue Generation Role</p> <p>Status by Service Role</p>	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/
Business Impact by Role	This dashboard shows the successful attacks on systems by asset category (business and data roles).	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/
Security Activity Statistics	This dashboard displays an overview of common attackers, targets, protocols, and activity by time.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Executive View	<p>This dashboard provides an overview of the network with respect to attacked systems status by asset location, business role, and worm activity.</p> <p>More detailed information is available from the follow-on dashboards in the Operational Summaries/Executive View Details group:</p> <p>Attacked or Compromised Systems</p> <p>Business Impact by Location</p> <p>Business Impact by Role</p> <p>Business Roles</p> <p>Worm Infected Systems</p> <p>This dashboard uses the following data monitors:</p> <p>Business Impact by Role - Successful Attacks</p> <p>Business Impact by Location - Successful Attacks</p> <p>Status by Business Role</p> <p>Worm Infected Systems</p>	Dashboard	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Worm Infected Systems	<p>This dashboard displays the number of systems infected by worms.</p> <p>More detailed information is available from the follow-on dashboards in the Detail/Attackers/Worm Outbreak group:</p> <p>Worm Outbreak</p> <p>Worm Spread Geo View</p> <p>This dashboard uses the following data monitors:</p> <p>Worm Infected Machines</p>	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/
Attacked or Compromised Systems	This dashboard shows targets and attackers with the attacks as nodes, and the top ten categories, by volume, of the event stream.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/
Business Impact by Location	This dashboard shows successful attacks on systems by asset location.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/
Security Intelligence Status Report	<p>This report displays four charts and six tables. The first chart gives an hourly breakdown of the event counts by agent severity. The three tables below the Event Count by Agent Severity chart show the top events, top attacks and top triggering rules. The three charts below the tables show the top attackers, top targets, and top target ports. The three tables at the bottom of the page show the number of cases added and notifications sent, along with a list of assets and the vulnerabilities used to compromise them.</p>	Report	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
<b>Library Resources</b>			
Worm Infected Systems	This active list is automatically populated by rules that have detected worm activity on a given system.	Active List	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Address Spaces	This is a site asset category.	Asset Category	Site Asset Categories
Security Devices	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Service	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Data Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Business Role	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Role	This is a site asset category.	Asset Category	Site Asset Categories
Operations	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Revenue Generation	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Location	This is a site asset category.	Asset Category	Site Asset Categories
Development	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Infrastructure	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Top Attacker IPs	This data monitor shows the counts of attack events and groups them by attacker IP address.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics
Status by Infrastructure Role	This data monitor displays the last state (Compromised, Attacked, or Resolved) of targets in the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Computer and the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network asset lists.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Business Roles/
Events per Address Space	This data monitor shows the count of events for each type of address space, such as public, private, and so on.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Top Connectors	This data monitor provides a list of the top ten ArcSight SmartConnectors reporting events, minute-by-minute within the last 60 minutes, showing the connector name and ID (Agent Name and Agent ID fields), the total number of events reported, and a breakdown of the reported events by priority.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Attacked or Compromised Systems	This data monitor displays the status of attacked or compromised systems.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Executive View/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Status by Development and Operations Roles	This data monitor displays the last state (Compromised, Attacked, or Resolved) of targets in the Site Asset Categories/Business Impact Analysis/Business Role/Development and the Site Asset Categories/Business Impact Analysis/Business Role/Operations asset lists.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Business Roles/
Status by Security Device Role	This data monitor displays the last state (Compromised, Attacked, or Resolved) of targets in the Site Asset Categories/Business Impact Analysis/Business Role/Security Devices asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Business Roles/
Worm Infected Machines	This data monitor shows the systems exhibiting the most worm-related traffic events.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Event Counts by Hour	This data monitor collects the count of events at each priority level for each hour for the last 24 hours.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Application Protocol Event Counts	This data monitor tracks the application protocol events by customer resource. The data monitor updates every 30 seconds. It uses 12 samples of five-minute intervals, for a time range of one hour. The data monitor requires a minimum of ten events to maintain a group (aggregated event counts are used when available).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Recent Events	This data monitor shows the last 15 significant events.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/



**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Worm Infected Systems	This data monitor displays the status of systems that have been infected in the course of a worm outbreak.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Worm Infected Systems
Status by Business Role	This data monitor displays the status of systems by Business Role, showing whether the target system has been attacked or compromised.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Executive View/
Top Target IPs	This data monitor shows the counts of attack events and groups them by the target IP address.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics
Successful Inbound Attacks	This resource has no description.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Successful Inbound Attacks/
Business Impact by Location - Successful Attacks	This data monitor displays the number of successful attacks on systems within each asset location.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Executive View/
Top Categories	This data monitor shows the top category of events over the last hours.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics
Status by Revenue Generation Role	This data monitor displays the last state (Compromised, Attacked or Resolved) of targets in the Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Business Roles/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Status by Service Role	This data monitor displays the last state (Compromised, Attacked or Resolved) of targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Business Roles/
Top Transport Protocols	This data monitor shows the number of events related to each transport protocol over the last hour.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Business Impact by Role - Successful Attacks	This data monitor displays a count and priority of the systems attacked by Business and Data Role.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/Executive View/
IDS	This field set displays useful fields for evaluating events from various firewall devices.	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Security	This field set contains several fields that are formatted to show more detailed information for security-related fields without needing to use the event inspector.	Field Set	ArcSight System/Event Field Sets/Active Channels
Virus Information	This field set displays useful fields for evaluating anti-virus events.	Field Set	ArcSight Foundation/Common/Anti-Virus

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Business Impact Analysis	This field set includes:  End Time  Business Role  Data Role  Attacker Zone Name  Target Host Name  Category Significance  Category Outcome  Priority	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight System/Event Field Sets/Active Channels
Worm Outbreak	This filter retrieves events with the name Worm Outbreak Detected and type Correlation.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Status by Business Role	This filter returns events with the names Compromise/Attempt, Compromise/Success, Hostile/Attempt, or Hostile/Success with target asset IDs that are associated with the Site Asset Categories/Business Impact Analysis/Business Role asset category hierarchy.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Business Role - Development and Operations	This filter returns the target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Development or the Site Asset Categories/Business Impact Analysis/Business Role/Operations Asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Attacked or Compromised Systems	<p>This filter retrieves events that have one of the following names:</p> <p>Compromise - Success</p> <p>Compromise - Attempt</p> <p>Hostile - Success</p> <p>Hostile - Attempt</p> <p>These events are generated by the rules of that name for use in the Attacked or Compromised Systems data monitor.</p>	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Business Role - Service	This filter returns the target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Service Asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/
Inbound Attacks	This filter identifies events that have a significance of compromise or hostile, and an outcome of success that are passing into the network.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Business Role - Infrastructure	This filter returns the target asset IDs that have the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Computer or the Site Asset Categories/Business Impact Analysis/Business Role/Infrastructure/Network asset categories associated with them.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Business Role - Revenue Generation	This filter returns the target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation Asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/
Worm Traffic	This filter selects events related to successful worm activity on a network.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Business Role - Security Devices	This filter returns the target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Security Devices Asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/
Successful Attacks	This filter detects events that have a significance of Compromise or Hostile, and an outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
SIS-Top Firing Rules Table Query	This query returns the event name and sums the aggregated event count where the type is Correlation for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Event Count by Agent Severity Chart Query	This query returns the date, agent severity, and the number of events for each agent severity level for that day/hour for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
SIS-Top Attacks Table Query	This query returns the event name and sums the aggregated event count for events that have a category significance of Compromise or Hostile, for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Cases Added Table Query	This query returns the stage, consequence severity, and a count of the cases with that pairing for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Top Targets Chart Query	This query returns the target zone name, target address, and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Top Events Table Query	This query returns the event name and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Assets Compromised Table Query	This query returns the target asset name, vulnerability external ID (the vulnerability name), and a sum of the number of events reported for that asset/vulnerability pair for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Notifications Sent Table Query	This query returns the group name, escalation level, acknowledgement status, and a count of the notifications for these conditions for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/

**Resources that Support the Security Overview Group, continued**

Resource	Description	Type	URI
SIS-Top Attackers Chart Query	This query returns the attacker zone name, attacker address, and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
SIS-Top Target Ports Chart Query	This query returns the target port and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/SIS/
Security Intelligence Status Template	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight Foundation/Intrusion Monitoring/SIS/
Revenue Generating Systems	This use case provides information about revenue generating systems.	Use Case	ArcSight Foundation/Intrusion Monitoring/Security Overview Group
Environment State	This use case provide information about environment state, such as application and OS status.	Use Case	ArcSight Foundation/Intrusion Monitoring/Security Overview Group
Business Impact Analysis	This use case provides business role related information.	Use Case	ArcSight Foundation/Intrusion Monitoring/Security Overview Group
Regulated Systems	This use case provides information about regulated systems.	Use Case	ArcSight Foundation/Intrusion Monitoring/Security Overview Group



## Targets

The Targets resources provide security information focused on target information.

- The By Port or Protocol content provides views of targets by target port. The protocol information can often be derived by the port number.
- The Target Counts content provides views of attackers from various perspectives: reporting device, target host, target port, ArcSight priority, and so on.
- The Targets in Lists content gives a view of targets that are in one or more of the ArcSight Core Priority Formula lists, which specify hit, scanned, or compromised.
- The Top and Bottom 10 content provides views of targets by using top and bottom 10 lists. The bottom 10 lists are useful for tracking the attackers who are trying to avoid detection by using the low-and-slow method (low volume over a long period of time), looking for a particular target.

The following device types can supply events that apply to the Targets resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems

## Targets Resources

The following table lists all the resources in the Targets group.

### Resources that Support the Targets Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Service-Email Attacks	This dashboard provides information about email attack activity. The dashboard uses the Top 10 Email Service Targets and the Email Service Attack Activity data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Service-Web Attacks	This dashboard provides information about web attack activity. The dashboard uses the Top 10 Web Service Targets and the Web Service Attack Activity data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/
Service-Database Attacks	This dashboard provides information about database attack activity. The dashboard uses the Top 10 Database Service Targets and the Database Service Attack Activity data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/
Service-Communications Attacks	This dashboard provides information about communications service attack activity. The dashboard uses the Top 10 Communications Service Targets and the Communications Service Attack Activity data monitors.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/
Critical Asset Monitoring	This resource has no description.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Service Attacks	<p>This dashboard provides an overview on service attack activity for web, email, database, and communications services. More detailed information is available from the follow-on dashboards in the Detail/Targets/Service Assets group:</p> <p>Service-Communications Attacks</p> <p>Service-Database Attacks</p> <p>Service-Email Attacks</p> <p>Service-Web Attacks</p> <p>This dashboard uses the Web Service Attack Activity, Email Service Attack Activity, Communications Service Attack Activity, and Database Service Attack Activity data monitors.</p>	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/
Successful Inbound Attacks	This resource has no description.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/
Top N Attack Signatures Targeting Windows Assets	This report displays the top attack signatures (event names) seen on the network affecting assets running a Microsoft operating system.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Top N Targets (Bar Chart)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Recent Activity Affecting Target Assets in Scanned List	This report displays the amount and type of activity related to assets in the Scanned List active list.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Targets in Scanned List	This report enumerates all the entries in the Scanned List active list and shows which entries have been recently modified (by comparing the creation time and last modified time).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Top Target Ports Chart	This report shows the target port and the sum of the aggregated event count for events matching the Attack Events filter where the target port is set.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/
Target Counts by ArcSight Priority	This report displays the priority, target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Target Counts by Attacker	This report displays the attacker zone name, attacker address, target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Top N Targets (Table)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Targets in Compromised List	This report displays the entries in the Compromised List active list and shows which entries have been recently modified (comparing the creation time and last modified time).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Recent Activity Affecting Target Assets in Compromised List	This report displays the customer name, zone name, address, event name, and the number of occurrences of events targeting assets in the Compromised List active list. This report is intended to show the amount and type of activity related to assets in the list.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Target Port Counts	This report displays the target zone name, the target address, the event name, and the sum of the aggregated event count for events matching the Attack Events filter where the target port is selected by the target port parameter, which defaults to 80.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/
Top N Targets (3D Pie Chart)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Top Targets	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Top N Targets (Pie Chart)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Bottom N Targets	This report displays the least targeted systems of those that have been attacked.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Top N Attacked Assets in North America	This report displays the attacked assets categorized as being in North America. Note: This report does not populate all values when running in Turbo Mode Fastest.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Targets in Hit List	This report enumerates all the entries in the Hit List active list and shows which entries have been recently modified (by comparing the creation time and last modified time).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Top Alert Destinations	This report shows the top IDS and IPS alert destinations per day.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Device Type/IDS/
Top N Targets (Table and Chart)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
By User Account - Compromised - Access	This report displays a table of events showing the Category Outcome, Target Zone Name, Target Address, Attacker User Name, Target User Name, Target Host Name, Target Process Name, and the sum of the Aggregated Event Count for events where the Attacker or Target User Name is in the Compromised User Accounts active list, the Target Address is set and the event has the Category Behavior of /Authentication/Verify.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/User Accounts/
Target Counts by Target Port	This report displays the target zone name, target address, target port, and the sum of the aggregated event count for events matching the Attack Events filter where the target port is not null.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/
By User Account - Compromised - All Activity	This report displays a table showing the category outcome, end time (by hour), target user name, attacker user name, target zone name, target address, and event name for events where the attacker or target user name is in the Compromised User Accounts active list.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/User Accounts/
Target Counts by Device	This report displays the device zone name, device address, target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/

### Resources that Support the Targets Group, continued

Resource	Description	Type	URI
Target Counts by Event Name	This report displays the event name, target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Recent Activity Affecting Target Assets in Hit List	This report displays the amount and type of activity related to assets in the Hit List active list.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Top N Targets (Inverted Bar Chart)	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
<b>Library Resources</b>			
Hit List	This Active List contains hosts targeted by a potential attacker.	Active List	ArcSight System/Targets
Suspicious List	This Active List contains hosts which have performed suspicious activity, either on the local system or over the network.	Active List	ArcSight System/Threat Tracking
Compromised List	This Active List contains hosts that may have been compromised by an attack.	Active List	ArcSight System/Threat Tracking
Compromised User Accounts	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
Scanned List	This Active List contains hosts that have been scanned by a potential attacker.	Active List	ArcSight System/Targets



**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
High	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Database	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role/Service
High	The unauthorized modification of destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality
Email	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role/Service
Microsoft	This is a site asset category.	Asset Category	Site Asset Categories/Operating System
Web	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role/Service
Dark	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Criticality	This is a system asset category.	Asset Category	System Asset Categories
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
North America	This is a site asset category.	Asset Category	Site Asset Categories/Location
High	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	Asset Category	Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality
Communications	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role/Service
Very High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Critical Target Assets Port Anomalies	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring/
Top 10 Email Service Targets	This data monitor displays the number of events affecting the top ten targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Email asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Email/
Critical Asset Group Count	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring/
Critical Attacker Assets	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Attacks	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring
Database Service Attack Activity	This data monitor displays the number of events affecting targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Database asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Database/
Web Service Attack Activity	This data monitor displays the number of events affecting targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Web asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Web Attacks/
Top Attackers Targeting Critical Assets	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring/
Critical Target Assets	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring/
Communications Service Attack Activity	This data monitor displays the number of events affecting targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Communications asset List	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Communications/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Top 10 Database Service Targets	This data monitor displays the number of events affecting the top ten targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Database asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Database/
Top 10 Communications Service Targets	This data monitor displays the number of events affecting the top ten targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Communications asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Communications/
Successful Inbound Attacks	This resource has no description.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Successful Inbound Attacks/
Critical Target Assets Event Graph	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Critical Asset Monitoring/
Top 10 Web Service Targets	This data monitor displays the number of events affecting the top ten targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Web asset list.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Assets/Service-Web Attacks/
Email Service Attack Activity	This data monitor displays the number of events affecting targets in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Email asset list	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Service Attacks
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Services - Web Service	This filter identifies target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Web Service asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/Services/
Very High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very High criticality.	Filter	ArcSight System/Core/Threat Level Filters
Services - Database Service	This filter identifies target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Database asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/Services/
High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a High criticality.	Filter	ArcSight System/Core/Threat Level Filters
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
Inbound Attacks	This filter identifies events that have a significance of compromise or hostile, and an outcome of success that are passing into the network.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Critical Target Asset Priority gt 6	This filter identifies non-ArcSight events in which the priority is greater than 6, the attacker address is set, and the target asset ID matches either the High Criticality Assets or Very High Criticality Assets filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Asset Criticality/
Critical Target Asset	This filter identifies non-ArcSight events in which the attacker address is set and the target asset ID matches either the High Criticality Assets or Very High Criticality Assets filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Asset Criticality/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Base events.	Filter	/All Filters/ArcSight Core Security/IDS-IPS Monitoring
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Attacks Targeting Assets	This resource has no description.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Critical Asset (High or Very High) Target Port Not Null	This filter identifies non-ArcSight events in which the target port is set and the target asset ID matches either the High Criticality Assets or Very High Criticality Assets filter.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Asset Criticality/
Critical Attacker Assets Priority gt 6	<p>This filter identifies events in which the priority is greater than 6 and the attacker asset ID is in one of the following groups:</p> <p>/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/High</p> <p>/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/High</p> <p>/All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/High</p> <p>/All Asset Categories/System Asset Categories/Criticality/High</p> <p>/All Asset Categories/System Asset Categories/Criticality/Very High</p>	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Asset Criticality/
Services - Communications Service	This filter identifies target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Communications asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/Services/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Services - Email Service	This filter identifies the target asset IDs that are in the Site Asset Categories/Business Impact Analysis/Business Role/Service/Email asset list.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/Business Roles/Services/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Top 10 Targets	This report shows the top ten targets in a chart.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Device Type/IDS/
Targets in Scanned List	This query returns the customer name, zone name, address, creation time, and last modified time of entries in the Scanned List active list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Top 10 Attacked Assets in North America	This query returns the target zone and target asset name from events where the event is an attack event and the target asset ID is in /All Asset Categories/Site Asset Categories/Location/North America. Note: This query does not populate all values when running in Turbo Mode Fastest.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/



**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
By User Account - Compromised - Access	This query returns the category outcome, target zone name, target address, attacker user name, target user name, target host name, target process name, and the sum of the aggregated event count for events where the attacker or target user name is in the Compromised User Accounts active list, the Target Address is set, and the event has the category behavior /Authentication/Verify.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/User Accounts/
Target Counts by ArcSight Priority	This query returns the priority, target zone name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Top 10 Attack Signatures targeting Windows Assets	This query returns the top attack signatures (event names) on the network affecting assets running a Microsoft operating system.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Targets in Hit List	This query returns the customer name, zone name, address, creation time, and last modified time of entries in the Hit List active list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Top Alert Destinations	This query returns the count of IDS and IPS alerts by destination address, zone, device vendor, and device product.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Device Type/IDS/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Top 10 Targets	This query returns the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter used in the following reports: Top N Targets, Top N Targets (3D Pie Chart), Top N Targets (Bar Chart), Top N Targets (Inverted Bar Chart), Top N Targets (Pie Chart), Top N Targets (Table and Chart), and Top N Targets (Table).	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Bottom 10 Targets	This query returns the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Top and Bottom 10/
Recent Activity Affecting Target Assets in Scanned List	This query returns events targeting assets in the Scanned List active list, selecting the customer name, zone name, address, event name, and a count of the events.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Target Port Counts	This query returns the target zone name, target address, event Name, and the sum of the aggregated event count for events matching the Attack Events filter where the target port is selected by the Target Port parameter, which defaults to 80.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Recent Activity Affecting Target Assets in Compromised List	This query returns events targeting assets in the Compromised List active list, selecting the customer name, zone name, address, event name, and a count of the events.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
By User Account - Compromised - All Activity	This query returns the category outcome, end time (by Hour), target user name, attacker user name, target zone name, target address, and event name for events where the attacker or target user name is in the Compromised User Accounts active list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/User Accounts/
Target Counts by Attacker	This query returns the attacker zone name, attacker address, target zone name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Targets in Compromised List	This query returns the customer name, zone name, address, creation time, and last modified time of entries in the Compromised List active list.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Target Counts by Target Port	This query returns the target zone name, target address, target port and the sum of the aggregated event count for events matching the Attack Events filter where the target port is not null.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Target Counts by Device	This query returns the device zone name, device address, target zone name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Top Target Ports Chart	This query returns the target port and the sum of the aggregated event count for events matching the Attack Events filter where the target port is set.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/By Port or Protocol/
Target Counts by Event Name	This query returns the event name, target zone name, target address and the sum of the aggregated event count for events matching the Attack Events filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Target Counts/
Recent Activity Affecting Target Assets in Hit List	This query returns events targeting assets in the Hit List active list, selecting the customer name, zone name, address, event name, and a count of the events.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/Targets in Lists/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Simple Chart Portrait	This template is designed to show one chart. The orientation is portrait.	Report Template	ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	ArcSight System/1 Chart/Without Table

**Resources that Support the Targets Group, continued**

Resource	Description	Type	URI
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table

## Vulnerability View

The Vulnerability View resources provide information about assets and their vulnerabilities, with an active channel that focuses on vulnerability scanner reports. These resources present two major reports that are a variation on the list of assets and the list of vulnerabilities.

Running the scanner reports can produce reams of output. Scanner reports are considered sensitive, so not every user should have access to these resources. For tips on restricting access to these resources, see ["Restricting Access to Vulnerability View Reports" on page 14](#).

The following device types can supply events that apply to the Vulnerability View resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Vulnerability scanners

## Vulnerability View Resources

The following table lists all the resources in the Vulnerability View group.

### Resources that Support the Vulnerability View Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Vulnerability Events	This active channel shows events received during the last two hours that are associated with a known vulnerability. The active channel includes a sliding window that displays the last two hours of event data.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Vulnerability Scanner Events	This active channel shows the events selected by the Scanner Events filter over the last hour, using the Vulnerability Scanner field set, which shows the description of the scanner event, the zone and address of the asset for which the vulnerability is being reported, and the scanner information, vendor, product and scanning host, reporting the vulnerability for that asset.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
Asset Vulnerability List	This report displays each asset (by zone) and all the vulnerabilities that have been reported for the asset. Note: This is an exhaustive list that can get extremely large.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Vulnerability View/
Daily Top 10 Vulnerabilities in Events Trend	This report shows the top ten most frequently detected vulnerabilities per day for the last seven days (by default). A line chart shows the count of each vulnerability exploit attempt per day. A line crossing several days indicates that the exploit was attempted several times each day. Single points are indicative of frequent exploit attempts that either occurred only on that day or were overshadowed by the volume of other exploit attempts on the other days. The table shows the same data as the chart in a reference format.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Vulnerabilities in Events by Zone	This report shows the vulnerability event counts seen on the network, by zone and shows a breakdown of the events by priority.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Top Vulnerabilities in Events Trend	This report displays the most frequent vulnerability exploit attempts on the network showing the vulnerabilities that are being targeted across the network in the last day or so. Use this report to gain a better understanding of the current threat activity.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Vulnerabilities and Assets	This report shows each vulnerability that has been reported for any asset and all the assets, by zone, affected by the vulnerability. Note: This is an exhaustive list that can get extremely large.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Vulnerability View/
Top N Vulnerabilities on Assets	This report displays the most frequent vulnerability exploit attempts against the network. This data is collected from the Asset Counts by Vulnerability trend. This trend is a snapshot trend of the assets taken once per week.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
<b>Library Resources</b>			
Vulnerability	<p>This field set shows the following columns:</p> <p>End Time</p> <p>Name</p> <p>Attacker Address</p> <p>Target Address</p> <p>Priority</p> <p>Vulnerability Resource</p> <p>Device Vendor</p> <p>Device Product</p>	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/



**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Vulnerability Scanner	<p>This field set shows the following columns:</p> <p>End Time</p> <p>Name</p> <p>Target Zone Resource</p> <p>Target Address</p> <p>Priority</p> <p>Device Vendor</p> <p>Device Product</p> <p>Device Host Name</p>	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Scanner Events	<p>This filter identifies events from network vulnerability scanners, where the events are defined as:</p> <p>Category Behavior = /Found/Vulnerable</p> <p>Category Device Group = /Assessment Tools</p> <p>Category Technique StartsWith /Scan</p> <p>Category Technique Contains vulnerability</p> <p>This filter is used by the Vulnerability Scanner Events active channel.</p>	Filter	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
Events with Vulnerabilities	<p>This filter identifies events in which the vulnerability field has been populated. The vulnerability field is populated when an event that attempts to exploit the vulnerability targets an asset that has had that vulnerability reported by a security scanner.</p>	Filter	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Vulnerabilities and Assets	This query returns the vulnerability, the asset zone, the asset address, the asset ID, the asset host name, and the count of the asset ID to get an exhaustive list of the assets and associated vulnerabilities. The asset ID count is used to retrieve assets that might not yet have any vulnerabilities reported. This query is used by the Asset Vulnerability Lists and Vulnerabilities and Assets reports, to provide two different views of the assets and vulnerabilities. Schedule the reports to run periodically to track changes in assets.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Vulnerability View/
Vulnerabilities in Events by Zone (Chart Query)	This query returns the zone, vulnerability name, and sums the aggregated event count for events matching the Events with Vulnerabilities filter to provide data for the Top N Vulnerabilities by Zone chart in the Vulnerabilities in Events by Zone report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Top 10 Daily Vulnerabilities in Events on Trend	This query on the Prioritized Vulnerability Events by Zone trend retrieves the top ten daily vulnerability events (by sum of the aggregated event count) each day. The data is used to populate the Top 10 Daily Vulnerability Events trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/Trend Queries/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Prioritized Vulnerabilities in Events by Zone	This query returns the zone, vulnerability name, priority, and sums the aggregated event count for events matching the Events with Vulnerabilities filter to provide data for the Top N Vulnerabilities by Zone with Priority table in the Vulnerabilities in Events by Zone report. This query also provides data for the Prioritized Vulnerability Events by Zone trend.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Vulnerabilities (by Asset Counts) on Trend	This query on the Asset Counts by Vulnerability trend returns the vulnerability and the sum of the assets affected by the vulnerability for the Top N Vulnerabilities on Assets report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Assets Counts by Vulnerability Trend	This query populates the Asset Counts by Vulnerability trend. It collects the vulnerability and the number of assets for which the vulnerability is reported. The query returns the most widely reported vulnerabilities in descending order, to show the most common vulnerabilities exposed on the network.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/Trend Queries/
Top N Vulnerabilities in Events on Trend	This query polls the Prioritized Vulnerability Events by Zone trend, returning the vulnerability name and the sum of the aggregated event count for use in the Top Vulnerabilities in Events Trend report.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Top 10 Daily Vulnerability Events on Trend	This query on the Top 10 Daily Vulnerability Events trend returns the date via a dependent variable (dvDate), and the sum of the aggregated event count for use in the Daily Top 10 Vulnerabilities in Events Trend report. The Top 10 Daily Vulnerability Events trend includes only ten events per day, and setting the row limit for this trend by a multiple of 10 will provide data for that many days. For example, setting the row limit to 70 will give the top 10 vulnerabilities per day for the last 7 days.	Query	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/Trend Queries/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight System/1 Chart/With Table
Prioritized Vulnerability Events by Zone	This trend stores the target zone name, the vulnerability name, the priority, and the sum of the aggregated event count to determine the top vulnerability events in a given time period. The trend runs queries once a day, collecting the top 1000 events. This allows the determination of the top ten most frequent vulnerability exploit attempts per day, and can give a reasonable view of the top ten attempts for the past week, or possibly the last month.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/

**Resources that Support the Vulnerability View Group, continued**

Resource	Description	Type	URI
Top 10 Daily Vulnerability Events	This trend collects daily information on the top ten vulnerabilities of the previous day. The trend uses the Top 10 Daily Vulnerabilities in Events on Trend query to retrieve the top ten events from the Prioritized Vulnerability Events by Zone trend for use in the Daily Top 10 Vulnerabilities in Events Trend report. The trend query is set up to only retrieve the top ten vulnerabilities, once per day.	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/
Asset Counts by Vulnerability	This trend collects the top 1000 vulnerabilities reported affecting the most assets on the network to give a view of which vulnerabilities represent the highest risk, by vulnerability exposure, on a weekly basis (assuming that the vulnerability scanner is scanning once per week). Adjust the timing of this trend and the report time range for more accuracy. A count with a blank vulnerability means that a number of assets do not have any vulnerabilities associated with them. You can locate these assets by reviewing the Vulnerabilities and Assets report (the blank vulnerability should have the zones, addresses, and host names of the assets with no reported vulnerabilities listed at the end of the report).	Trend	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Vulnerability View/

## Worm Outbreak

The Worm Outbreak resources provide information about worm activity and the affect a worm has had on the network.

The following device types can supply events that apply to the Worm Outbreak resource group:

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Operating systems
- Vulnerability scanners
- Anti-virus Systems

## Worm Outbreak Resources

The following table lists all the resources in the Worm Outbreak group.

### Resources that Support the Worm Outbreak Group

Resource	Description	Type	URI
<b>Monitor Resources</b>			
Worm Outbreak	This dashboard provides a view of worm activity across the network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/
Worm Outbreak Overview	This dashboard provides a view of worm activity across the network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/
Worm Spread Geo View	This dashboard displays a world map showing worm activity affecting the network.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/

**Resources that Support the Worm Outbreak Group, continued**

Resource	Description	Type	URI
Worm Infected Systems	This report presents a table of systems that have been infected by a worm. The table is sorted by the Attacker Zone Name, then by the Attacker Host Name and finally by the Attacker Address (for cases where the system does not have a host name). You can change the start and end times of the event query, and the row limit (to show more or fewer systems). You can also use the Filter By parameter to create an additional filter to limit the report to specific systems. Changing the Filter By parameter causes the query to select events that match both the selected filter and the Worm Traffic filter (Worm Traffic AND <selected filter>).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/
<b>Library - Correlation Resources</b>			
Blaster DDOS From Infected Host	This rule detects a Distributed Denial Of Service (DDOS) attack (Blaster) originating from an infected host. This rule detects DoS events targeting a windowsupdate.com host, either coming from a host in the Attackers/Untrusted List active list or from a host in the Targets/Compromised List active list. This means that a compromised target could be acting as an attacker. In this case, this host is infected. This rule only requires one such event, and the time frame is set to two minutes. After this rule is triggered, the categoryOutcome field is set to Success and the categorySignificance field is set to Hostile.	Rule	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/

**Resources that Support the Worm Outbreak Group, continued**

Resource	Description	Type	URI
Blaster Infected Host	This rule detects infected hosts by a Blaster worm. This rule looks for two events. The first event, the ExploitEvent, targets one of the following ports: 135, 139 or 445. The second event, the TftpEvent, targets the port 69 and uses UDP. Neither event comes from a host in the Attackers/Trusted List active list. To have a matching event, the Attacker-Target pair in the first event must match the swapped Target-Attacker pair in the second event. This rule requires one matching occurrence, and the time frame is set to two minutes. On the first occurrence, a notification is sent to the Analysts, the target of ExploitEvent is added to the Worm Infected Systems active list. The correlation event from the rule triggering is caught by the Hostile - Success rule.	Rule	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Possible Internal Network Sweep	This rule detects a single host trying to communicate with at least ten other hosts on the same target port within the network, within a minute. This rule, combined with a spike in target port activity by the same host, results in the worm outbreak detected rule being triggered.	Rule	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Possible Outbound Network Sweep	This rule detects a single host trying to communicate with at least ten other hosts on the same target port outside the network within a minute. This rule, combined with a spike in target port activity by the same host, results in the worm outbreak detected rule being triggered.	Rule	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
<b>Library Resources</b>			



**Resources that Support the Worm Outbreak Group, continued**

Resource	Description	Type	URI
Compromised List	This Active List contains hosts that may have been compromised by an attack.	Active List	ArcSight System/Threat Tracking
Worm Infected Systems	This active list is automatically populated by rules that have detected worm activity on a given system.	Active List	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	Active List	ArcSight System/Attackers
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Domain Name Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Proxy	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Worm Propagation by Host	This data monitor shows the spread of worm activity throughout the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Worm Propagation by Zone	This data monitor shows the spread of worms across network zones.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Worm Infected Systems	This data monitor displays the status of systems that have been infected in the course of a worm outbreak.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Worm Infected Systems

**Resources that Support the Worm Outbreak Group, continued**

Resource	Description	Type	URI
Worm Spread	This data monitor tracks worm activity affecting the network for display on a world map.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Spread Geo View/
Worm Activity Status	This data monitor shows the most recent events related to worm activity in the network zones.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Target Port Activity by Attacker	This data monitor is used in conjunction with the Worm Outbreak detected rule and the possible network sweep rule to detect worm outbreaks before an IDS signature is released.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Worm Outbreak	This filter retrieves events with the name Worm Outbreak Detected and type Correlation.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Target Port Activity By Attacker	This filter selects events where the source address is available, the target (destination) port is available but is not the ArcSight port (8443), and the source is not a DNS, email, or proxy server.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Worm Geo Filter	This filter is used by the Worm Spread data monitor in the Worm Spread Geo View dashboard to graph worm related events between systems on a world map. Worm related events are defined here as a category object of /Vector/Worm or /Host/Infection/Worm, or a category technique of /Code/Worm. For the event to be graphed, either the attacker or the target systems need to have their geographic longitudes and latitudes set (they must be NOT NULL).	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/

**Resources that Support the Worm Outbreak Group, continued**

Resource	Description	Type	URI
Worm Infected Systems	This resource has no description.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Internal to Internal Events	This filter retrieves events internal to the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Worm Traffic	This filter selects events related to successful worm activity on a network.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
All Events	This filter matches all events.	Filter	ArcSight System/Core
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters
Worm Activity	This filter selects events related to all worm activity on a network.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Worm Infected Systems	This query returns the attacker zone name, attacker host name, and attacker address from events matching the Worm Traffic filter.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	ArcSight System/1 Table

## Send Documentation Feedback

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

### **Feedback on Intrusion Monitoring Standard Content Guide (ESM 6.8c)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arc-doc@hp.com](mailto:arc-doc@hp.com).

We appreciate your feedback!