

Standard Content Guide

Intrusion Monitoring

for ArcSight ESM 5.5

March 1, 2013



Standard Content Guide - Intrusion Monitoring

Copyright © 2013 Hewlett-Packard Development Company, L.P.

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.

The information contained herein is subject to change without notice. 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.

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

<http://www.arcsight.com/copyrightnotice>

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

This document is confidential.

Revision History

Date	Product Version	Description
03/01/2013	Intrusion Monitoring 5.5	Final revision for release.

Document template version: 2.1

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: Intrusion Monitoring Overview	7
What is Standard Content?	7
Standard Content Packages	8
Intrusion Monitoring Content	9
Chapter 2: Installation and Configuration	11
Installing the Intrusion Monitoring Package	11
Configuring Intrusion Monitoring Content	12
Modeling the Network	12
Categorizing Assets	13
Configuring Active Lists	13
Enabling Rules	14
Configuring the Network Management Filter	14
Configuring Notification Destinations	15
Configuring Notifications and Cases	15
Scheduling Reports	15
Restricting Access to Vulnerability View Reports	15
Configuring Trends	16
Chapter 3: Intrusion Monitoring Content	17
Alerts from IDS-IPS	19
Devices	19
Resources	19
Anti-Virus Activity and Status	22
Devices	22
Resources	22
Attack Rates	27
Devices	27
Configuration	27
Resources	27
Attackers	37
Devices	37
Resources	37
Business Impact Analysis	54

Devices	54
Configuration	54
Resources	54
DoS	59
Devices	59
Configuration	59
Resources	59
Environment State	66
Devices	66
Resources	66
Login Tracking	74
Devices	74
Configuration	74
Resources	74
Reconnaissance	95
Devices	95
Configuration	95
Resources	96
Regulated Systems	106
Devices	106
Configuration	106
Resources	106
Resource Access	109
Devices	109
Configuration	109
Resources	109
Revenue Generating Systems	119
Devices	119
Resources	119
SANS Top 5 Reports	122
Devices	122
Resources	122
SANS Top 20	129
Devices	129
Configuration	129
Resources	129
Security Overview	145
Devices	145
Configuration	145
Resources	145
Targets	155
Devices	155
Resources	155

Vulnerability View	168
Devices	168
Resources	168
Worm Outbreak	174
Devices	174
Resources	174
Appendix A: Upgrading Standard Content	179
Preparing Existing Content for Upgrade	179
Configurations Preserved During Upgrade	179
Configurations that Require Restoration After Upgrade	179
Backing Up Existing Resources Before Upgrade	180
Performing the Upgrade	180
Checking and Restoring Content After Upgrade	180
Verifying and Reapplying Configurations	181
Verifying Customized Content	181
Fixing Invalid Resources	181
Index	183

Chapter 1

Intrusion Monitoring Overview

This chapter discusses the following topics.

["What is Standard Content?" on page 7](#)

["Standard Content Packages" on page 8](#)

["Intrusion Monitoring Content" on page 9](#)

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.

The standard content is installed using a series of packages, some of which are installed automatically with the 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 System** content is installed automatically with the Manager and consists of 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.
- **ArcSight Administration** content is installed automatically with the Manager, and provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of content and components.
- **ArcSight Foundations** content (such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, NetFlow Monitoring, and Workflow) are presented as install-time options and 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.
- **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 are 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 are 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.
- ◆ Network filters are a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

Standard Content Packages

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

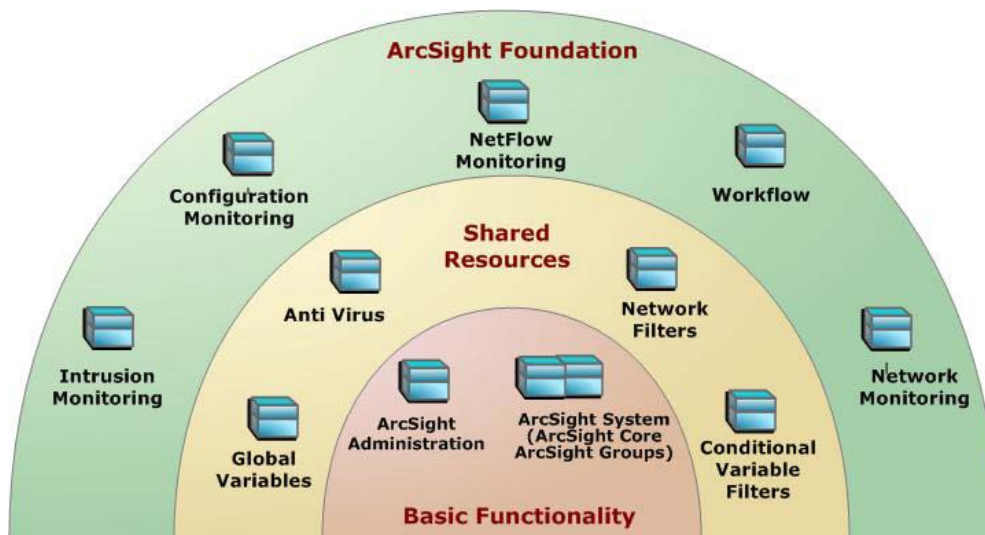


Figure 1-1 The ArcSight System and ArcSight Administration packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support ArcSight Administration and the ArcSight Foundation packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

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



The ArcSight Express package is present in ESM installations, but is not installed by default. The package offers an alternate view of the Foundation resources. You can install or uninstall the ArcSight Express package without impact to the system.



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; for example, zones. 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 System or ArcSight Administration content, refer to the *ArcSight Standard Content Guide - ArcSight System and ArcSight Administration*. 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.arcsight.com>).

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

[“Installing the Intrusion Monitoring Package” on page 11](#)

[“Configuring Intrusion Monitoring Content” on page 12](#)

For information about upgrading standard content, see [Appendix A, Upgrading Standard Content, on page 179](#).

Installing the Intrusion Monitoring Package

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

If you opted to exclude any packages at installation time, the package is imported into the ESM package view in the Navigator panel, but is not available in the resource view. The package icon in the package view will appear grey.

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

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

- 1 In the Navigator panel Package view, 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 In the Navigator Panel Package view, 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**.

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**.

- 4 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 package view, and can be re-installed at another time.

To delete a package and remove it from the Console and the database:

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

The package is removed from the Navigator panel package view.

Configuring Intrusion Monitoring Content

The list below shows the general tasks you need to complete to configure Intrusion Monitoring content with values specific to your environment.

- ["Modeling the Network" on page 12](#)
- ["Categorizing Assets" on page 13](#)
- ["Configuring Active Lists" on page 13](#)
- ["Enabling Rules" on page 14](#)
- ["Configuring the Network Management Filter" on page 14](#)
- ["Configuring Notification Destinations" on page 15](#)
- ["Configuring Notifications and Cases" on page 15](#)
- ["Scheduling Reports" on page 15](#)
- ["Restricting Access to Vulnerability View Reports" on page 15](#)
- ["Configuring Trends" on page 16](#)

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* or the ESM online Help. To learn more about the architecture of the ESM 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.

- Categorize all assets (or the zones to which the assets belong) that are internal to the network with the [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#) category.

Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as *Protected*.



Assets with a private IP address (such as 192.168.0.0) are considered *Protected* by the system, even if they are not categorized as such.

- Categorize all assets that are considered *critical* to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with the [/All Asset Categories/System Asset Categories/Criticality/High](#) or [Very High](#) category.

The asset categories most essential to basic event processing are those used by the Priority Formula to calculate an event's criticality. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.

Asset categories can be assigned 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 Console tools, refer to the *ArcSight Console User's Guide* or the ESM online Help.

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.

Enabling Rules

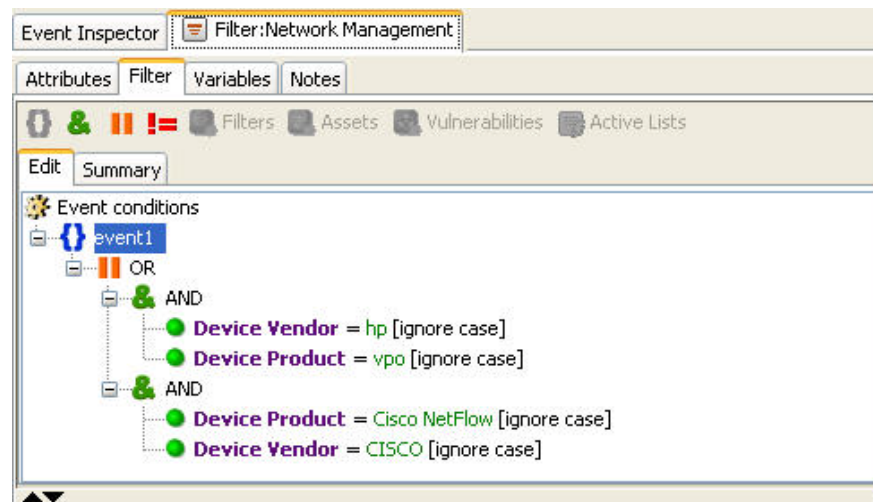
ESM rules trigger only if they are deployed in the [Real-Time Rules](#) group and are enabled. The Intrusion Monitoring rules are all deployed by default in the [Real-Time Rules](#) group and are also enabled.

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.

This filter is required by the Event Counts by Hour data monitor ([/All Data Monitors/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/Event Counts by Hour](#)).

Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in rules, see [Configuring Notifications and Cases](#), below.

Intrusion Monitoring rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. Refer to the *ArcSight Console User's Guide* or the ESM online Help 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, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group.

To enable rules to send notifications and open cases, first configure notification destinations as described in ["Configuring Notification Destinations" on page 15](#), 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* or the ESM online Help.

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 Intrusion Monitoring, 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* or the ESM online Help.

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**.



Caution

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 backfills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

For more information about trends, refer to the the *ArcSight Console User's Guide* or the ESM online Help.

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 19	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 22	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 27	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 37	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 54	The Business Impact Analysis resources provide information about which business areas are the victims of the most attack activity.
"DoS" on page 59	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 66	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 74	The Login Tracking resources provide information about user logins.

Resource Group	Purpose
"Reconnaissance" on page 95	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 106	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 109	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 119	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 122	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 129	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 145	The Security Overview resources provide information of interest to executive level personnel.
"Targets" on page 155	The Targets resources provide security information focused on target information.
"Vulnerability View" on page 168	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 174	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.

Devices

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

Resources

The following table lists all the resources in the Alerts from DS-IPS resource group and any dependant resources.

Table 3-1 Resources that Support the Alerts from IDS-IPS Group

Resource	Description	Type	URI
Monitor Resources			
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 for 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 in a chart and a table. The chart shows the top 10 device addresses with the highest counts. The 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/
Alert Counts by Port	This report shows the count of IDS and IPS alerts by destination port in a chart and a table. The chart shows the top ten ports with the highest counts. The table shows the list of all the counts sorted in descending order.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/

Resource	Description	Type	URI
Alert Counts by Severity	This report shows the total count of IDS and IPS alerts by severity (agent severity) in a chart and a table. The chart shows the count of alerts by severity. The 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) in a chart and a table. The chart shows the top ten alert counts. The table shows the list of all the counts sorted by descending order.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/
Library Resources			
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
All Events	Filter that 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 selects 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 selects 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/
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 selects the count of IDS and IPS alerts by severity (agent severity), device vendor, and device product.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/

Resource	Description	Type	URI
Alert Counts by Device	This query selects 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 selects the count of IDS and IPS alerts per hour.	Query	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/

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.

Devices

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

Resources

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

Table 3-2 Resources that Support the Anti-Virus Activity and Status Group

Resource	Description	Type	URI
Monitor Resources			
Virus Activity Statistics	This dashboard displays data monitors describing virus activity from two perspectives. 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/
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/
Virus Activity Overview	This dashboard displays data monitors describing 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/

Resource	Description	Type	URI
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/Common/Anti-Virus/
Top Infected Systems	This report displays summaries of the systems reporting the most infections in the previous day.	Report	ArcSight Foundation/Common/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/Common/Anti-Virus/
Virus Activity by Time	This report displays the malware activity by hour for the previous day by hour and priority.	Report	ArcSight Foundation/Common/Anti-Virus/
Update Summary	This report displays a summary of the results of anti-virus update activity by zones since yesterday.	Report	ArcSight Foundation/Common/Anti-Virus/
Library Resources			
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 Failure 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 systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable).	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 systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Anti-Virus Overview/

Resource	Description	Type	URI
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/
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/
Anti-Virus Events	This filter identifies events with the category device group of /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 Failure and the Category Behavior is /Found/Vulnerable.	Filter	ArcSight Foundation/Common/Anti-Virus/
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/

Resource	Description	Type	URI
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	Filter that 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 filter the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure and the Category Behavior is /Found/Vulnerable), and returns the host information and a count of the infections per host.	Query	ArcSight Foundation/Common/Anti-Virus/Top Infected Systems/
Failed Anti-Virus Updates	This query identifies the device vendor, device product target zone name, target host name, and target address and time (EndTime) from events that match the AV - Failed Updates filter.	Query	ArcSight Foundation/Common/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 Failure, and the Category Behavior is /Found/Vulnerable). This query returns the time, priority, virus activity, and a count of activity occurrences.	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/

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/Common/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 Failure and the Category Behavior is /Found/Vulnerable), and returns the host zone and a count of the infections per zone.	Query	ArcSight Foundation/Common/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/
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/Common/Anti-Virus/

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.

Devices

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

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

Configuration

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.

Resources

The following table lists all the resources in the Attack Rates resource group and any dependant resources.

Table 3-3 Resources that Support the Attack Rates Group

Resource	Description	Type	URI
Monitor Resources			
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/
Top 10 Attack Rate Statistics by Service	This dashboard provides 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.	Dashboard	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attack Rates/

Resource	Description	Type	URI
Customer Attack Rates by Service	This dashboard provides an overview of the attack rates by service. The overview 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 areas 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/
Attack Rates by Service and Zones	This dashboard displays an overview of the attack rates by service. The overview 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. The overview 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/

Resource	Description	Type	URI
Top 10 Attack Rate Statistics by Service and Zones	This dashboard provides a top ten view of the attack rates by service. The dashboard 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.	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/
Attack Rates by Service	This dashboard provides an overview of the attack rates by service. The overview 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 the counts of the events separated by priority. A detailed table shows the 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/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 detailed 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/

Resource	Description	Type	URI
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 detailed 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/
Library Resources			
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/

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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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 identified if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
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 identified 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 identified 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/

Resource	Description	Type	URI
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/
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/

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/
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).

Devices

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

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

Resources

The following table lists all the resources in the Attackers resource group and any dependant resources.

Table 3-4 Resources that Support the Attackers Group

Resource	Description	Type	URI
Monitor Resources			
Target Counts by Attacker Port	This report displays the attacker port, target zone name, target address, 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/
Denied Outbound Connections by Port	This report shows a summary of the denied outbound traffic by destination port in a chart and a table. The chart shows the top ten ports with the highest denied connections count. The reports lists all the ports sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
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 each user's connection durations 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/

Resource	Description	Type	URI
Denied Outbound Connections per Hour	This report shows a summary of the denied outbound traffic per hour in a chart and a table. The chart shows the total number of denied connections per hour for the previous day (by default). The 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 (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 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/
Top N Attacker Details	This report displays the priority, attacker zone name, attacker address, and the count of attack events (the category significance starts with Compromise or Hostile), in a chart and table format. 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 (the category significance starts with Compromise or Hostile), with a chart overview and a detailed table.	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 (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 in a chart and a table. The chart shows the total number of denied connections per hour for the previous day (by default). The table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/

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 in a chart and a table. The chart shows the top ten addresses with the highest denied connections count. The reports 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 (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 in a chart and a table. The chart shows the top ten addresses with the highest denied connections count. The reports lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Top Alert Sources	This report shows the top IDS and IPS alert sources per day in a chart and a table. The chart shows the top ten IDS and IPS alert source IP addresses. The 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 (the category significance starts with Compromise or Hostile).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Top and Bottom Attackers/

Resource	Description	Type	URI
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 (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 (the category significance starts with Compromise or Hostile).	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/Attacker Counts/
Bottom N Attack Sources	This report displays the attacker zone name and a sum of the count of attack events (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 in a chart and a table. The chart shows the top 10 ports with the highest denied connections count. The reports lists all the ports sorted by connection count.	Report	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/By Device Type/Firewall/
Library - Correlation Resources			
Traffic From Dark Address Space	This rule detects traffic originating from the Dark address space and adds the target address to the Hit active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/
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, and 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/

Resource	Description	Type	URI
Brute Force Logins	This rule detects non-application brute force login attempts. The rule looks for occurrences of login attempts or failures from sources that are not listed on a trusted active list. The rule triggers after five occurrences 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/
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/

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 (that is, whenever a database, a service, or an 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/
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 repetitively blocked by the firewall. The rule monitors failure access. The rule triggers when ten events occur in 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/

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 looks for occurrences of login attempt or failure 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/
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 (that is, 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 on 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 set.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/
Windows Account Locked Out Multiple Times	This rule detects Microsoft Windows user account locked out events (Security:644). The rule triggers if the Locked Count for that user account in the Windows Locked Out Accounts active list is equal or greater than five. On the first event, the category significance is set to Informational/Warning.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/

Resource	Description	Type	URI
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/
Application Brute Force Logins	This rule detects application brute force login attempts with the same user name from the same attacker. It looks for 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 in 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/
Multiple Login Attempts to Locked Windows Account	This rule detects Microsoft Windows login attempt events targeting locked out accounts (Security:531). The rule triggers when five events originating from the same host and targeting the same account occur within two minutes. On the first threshold, the category significance is set to Informational/Warning.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/
Notify on Successful Attack	This rule detects successful attacks. This rule looks for high priority (≥ 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 this action is disabled by default.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/

Resource	Description	Type	URI
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/
Suspicious Activity - Excess Suspicious Activity	This rule detects an excessive number of suspicious events between the same attacker/object 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/
Attack From Suspicious Source	This rule detects attacks coming from a source categorized as suspicious or untrusted and does not belong to Attackers/Trusted 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 List has category significance hostile and compromise. On the first event, the source address is added to the Hostile active list and 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 hostile list and the target to comprised list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/

Resource	Description	Type	URI
Windows Account Created and Deleted within 1 Hour	This rule detects Microsoft Windows account deletion events (Security:630). The rule triggers if the user account that is being deleted is in the Windows Created Accounts active list (by default, the active list TTL is set to one hour). On the first event, the user account is removed from the Windows Created Accounts active list and the category significance is set to Suspicious.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/
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 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 - Execute	This rule detects 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 operating system, service, or application. The rule triggers when the Execute_Attack event ends before the Execute event (that is, 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 list and the target is added to the Compromised list. This rule is triggered by applications, services, or operating systems.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Successful Attacks/

Resource	Description	Type	URI
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/
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/
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/
Multiple Windows Logins by Same User	This rule detects Microsoft Windows successful user login events. The rule triggers if the login count for that user in the Windows Login Count active list is equal or greater than five (by default, the TTL for the active list is one hour). On the first event, the category significance is set to Informational/Warning.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/

Library Resources

Resource	Description	Type	URI
Suspicious List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Hostile List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Hit List	This resource has no description.	Active List	ArcSight System/Targets
Compromised List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Compromised User Accounts	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from specific systems to other specific systems that have been determined to be not relevant to the rules that would otherwise fire on these events.	Active List	ArcSight System/Tuning
User-based Rule Exclusions	This active list contains target user information of specific users to be excluded from certain rule conditions where the rule tracks user activity.	Active List	ArcSight System/Tuning
Windows Locked Out Accounts	This active list stores the user ID, the user name, and the number of times a Windows account has been locked out. The Windows Account Locked Out rule adds user accounts to the list (or increment the count if the user account is already in the list). The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Infiltrators List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Windows Login Count	This active list stores the user ID, the user name, and the current number of workstations a Windows user is logged in to. The Successful Windows Login rule increments the count and the Successful Windows Logout rule decrements the count. The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers
Untrusted List	This resource has no description.	Active List	ArcSight System/Attackers
Repetitive Firewall Block List	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/

Resource	Description	Type	URI
Windows Created Accounts	This active list stores the user ID and the user name of the Windows accounts that have been created. The Windows Account Created rule adds user accounts to the list and the Windows Account Created and Deleted within 1 Hour removes user accounts from the list. The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/
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
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack 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/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Successful Windows Login	This filter detects successful Windows login events (Device Event Class ID = Security:528). The filter looks for the following types of logins: console (2), lock (7), and remote (10).	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
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	Filter that 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/
ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/

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/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Non-ArcSight Events	This resource has no description.	Filter	ArcSight System/Event Types
Top 10 Attackers	This report shows the top ten attackers in a chart.	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/
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/

Resource	Description	Type	URI
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 identifies 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/
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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
Top Users by Connection Count	This query identifies VPN events where 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/
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/
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.

Devices

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

Configuration

The Business Impact Analysis resource group requires the following configuration for your environment:

- 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 13](#).

Resources

The following table lists all the resources in the Business Impact Analysis resource group and any dependant resources.

Table 3-5 Resources that Support the Business Impact Analysis Group

Resource	Description	Type	URI
Monitor Resources			
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/

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/

Resource	Description	Type	URI
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/
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 displays a table and a chart showing 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/

Resource	Description	Type	URI
Business Role - Attempted Attacks	This report displays a chart and a table showing 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/
Library Resources			
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
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/
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	This filter detects hostile & compromise events relating to target assets within the Business Role, Data Role or Classification categories. The events match: - Non-ArcSight Internal Event - Target asset has a Business Impact Analysis Category - Priority > 5 - Category Significance StartsWith /Compromise or /Hostile The Business Role, Data Role and Classification categories are sub-categories of /All Asset Categories/Site Asset Categories/Business Impact Analysis.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types

Resource	Description	Type	URI
ASM Events	This resource has no description.	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	Filter that 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/

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.

Devices

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

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

Configuration

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

- Populate the [/ArcSight System/Tuning/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.

Resources

The following table lists all the resources in the DoS resource group and any dependant resources.

Table 3-6 Resources that Support the DoS Group

Resource	Description	Type	URI
Monitor Resources			
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 = /DoS, the Category Significance = /Compromise, the Category Outcome = /Success and the event MatchesFilter(Internal Target) .	Active Channel	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/

Resource	Description	Type	URI
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 trend 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/
Library - Correlation Resources			
Possible DoS on Hosts	This rule detects two conditions: a spike in events detected by the Inbound Event Spikes for Hosts data monitor, and an event describing either failure to communicate with the host mentioned in the first event or an event describing a host shut down. The rule detects two such events within three minutes. This aggregation is used to keep the rule from triggering too often if a host reboots or restarts its affected service quickly. On the first event, the rule triggers an event describing a successful Denial of Service compromise on the affected host.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/

Resource	Description	Type	URI
Possible DoS on Network	This rule detects two conditions: a spike in events detected by the Inbound Event Spikes for Networks data monitor, and an event describing either failure to communicate with hosts on the network zone mentioned in the first event. The rule detects six such events within one minute with six different hosts. This aggregation is used to determine whether the spike is for a specific host on the network or a possible Denial of Service attack against the entire network. On the first threshold (six such events), the rule triggers an event describing a successful Denial of Service compromise on the affected network zone.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Possible DoS on Services	This rule detects two conditions: a spike in events detected by the Inbound Event Spikes for Services data monitor, and an event describing either failure to communicate with a service on a host mentioned in the first event or an event describing a service shutdown. The rule triggers when there are two such events within three minutes. This aggregation is used to keep the rule from triggering too often if a host reboots or restarts its affected service quickly. On the first event, the rule triggers an event describing a successful Denial of Service compromise on the affected network zone.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
High Number of IDS Alerts for DoS	This rule detects Denial of Service (DoS) 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/DoS/
SYN Flood Detected by IDS or Firewall	This rule detects SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/
Library Resources			
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers

Resource	Description	Type	URI
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from specific systems to other specific systems that have been determined to be not relevant to the rules that would otherwise fire 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/
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/

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 identified if an event has an entry for the Application Protocol field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
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/

Resource	Description	Type	URI
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/
ASM Events	This resource has no description.	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) events.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack 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 identified 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 resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types

Resource	Description	Type	URI
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 identified 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/
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/
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.

Devices

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

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

Resources

The following table lists all the resources in the Environment State resource group and any dependant resources.

Table 3-7 Resources that Support the Environment State Group

Resource	Description	Type	URI
Monitor Resources			
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/

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 10 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/
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/

Resource	Description	Type	URI
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/
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/
Library Resources			
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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
Application Protocol is not NULL	This filter identified 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 resource has no description.	Filter	ArcSight System/Event Types
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
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 identified if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	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/

Resource	Description	Type	URI
Transport Protocol is not NULL	This filter identified 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/
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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.

Devices

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

Configuration

The Login Tracking resource group requires the following configuration for your environment:

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

Resources

The following table lists all the resources in the Login Tracking resource group and any dependant resources.

Table 3-8 Resources that Support the Login Tracking Group

Resource	Description	Type	URI
Monitor Resources			
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
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/
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/
Library - Correlation Resources			
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 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 list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/

Resource	Description	Type	URI
Successful Windows Logout	This rule detects Microsoft Windows successful user logout events. On the first event, the Login Count in the Windows Login Count active list is decremented, and the device and agent severity is set to Low.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Windows Account Locked Out	This rule detects Microsoft Windows user account locked out events (Security:644). On the first event, the user account is added in the Windows Locked Out Accounts active list, and the device and agent severity are set to Medium. If the user account is already in the active list, the Locked Count is incremented.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/
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 list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
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 list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
Successful Windows Login	This rule detects Microsoft Windows successful user login events. On the first event, the user account is added to the Windows Login Count active list, and the device and agent severity is set to Low. If the user is already in the active list, the Login Count is incremented.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/
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 list. This rule supports Cisco Secure ACS.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/

Resource	Description	Type	URI
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 list. This rule supports Cisco VPN products, Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Windows Account Created	This rule detects Microsoft Windows account creation events (Security:624). On the first event, the user account is added to the Windows Created Accounts active list, and the device and agent severity is set to Low.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/
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 list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
User VPN Session Started	This rule detects VPN user session start events, defined as a VPN access start event with user ID information. It then updates the User VPN Sessions list. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	Rule	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Library Resources			
User-based Rule Exclusions	This active list contains target user information of specific users to be excluded from certain rule conditions where the rule tracks user activity.	Active List	ArcSight System/Tuning
Windows Locked Out Accounts	This active list stores the user ID, the user name, and the number of times a Windows account has been locked out. The Windows Account Locked Out rule adds user accounts to the list (or increment the count if the user account is already in the list). The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/

Resource	Description	Type	URI
Windows Login Count	This active list stores the user ID, the user name, and the current number of workstations a Windows user is logged in to. The Successful Windows Login rule increments the count and the Successful Windows Logout rule decrements the count. The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Windows Created Accounts	This active list stores the user ID and the user name of the Windows accounts that have been created. The Windows Account Created rule adds user accounts to the list and the Windows Account Created and Deleted within 1 Hour removes user accounts from the list. The TTL is set to one hour by default.	Active List	ArcSight Foundation/Intrusion Monitoring/User Tracking/
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/
Top Users by Login Activity	This top 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/
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/
Top Users by Login Activity	This top 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/
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/
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/
Top Users by Login Activity	This top 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/
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/

Resource	Description	Type	URI
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 Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
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/
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 firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall/
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/
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/
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/

Resource	Description	Type	URI
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/
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/
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/
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/
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/
Successful Windows Logout	This filter identifies successful Windows logout events (Device Event Class ID = Security:538). The filter looks for the following types of logouts: console (2), lock (7), and remote (10).	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
VPN Events	This filter identifies events with the category device group of VPN.	Filter	ArcSight Foundation/Common/Device Class Filters/
Login Events	This filter identifies events with the category behavior of /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/

Resource	Description	Type	URI
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/
Successful Login Events	This filter identifies events with the category behavior of /Authentication/Verify and category outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/
Failed Login Events	This filter identifies events with the category behavior of /Authentication/Verify and category outcome of Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/
VPN Login Events	This filter identifies VPN events with the category behavior of /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Operating System Login Events	This filter identifies operating system events with the category behavior of /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
Failed Operating System Login Events	This filter identifies operating system events with the category behavior of /Authentication/Verify and category outcome of Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
ASM Events	This resource has no description.	Filter	ArcSight System/Event Types
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Successful Operating System Login Events	This filter identifies operating system events with the category behavior of /Authentication/Verify and category outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
Failed Network Login Events	This filter identifies events with the category behavior of /Authentication/Verify, category outcome of Failure, and category object starting with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/
Successful Network Login Events	This filter identifies events with the category behavior of /Authentication/Verify, category outcome of Success, and category object starting with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/
LockedCount is NULL	This filter identifies events in which the LockedCount is NULL. The LockedCount variable used in the Windows Account Locked Out rule and retrieves from the Windows Locked Out Accounts active list, the number of times a Windows account has been locked out.	Filter	ArcSight Foundation/Intrusion Monitoring/Conditional Variable Filters/

Resource	Description	Type	URI
Attacker User ID is NULL	This filter identifies events where the Attacker User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User/
LoginCount is NULL or 0	This filter identifies events in which the LoginCount is NULL or equal to 0. LoginCount is a variable used in the Successful Windows Login and Successful Windows Logout rules and retrieves the number of successful Windows logins from the Windows Login Count active list.	Filter	ArcSight Foundation/Intrusion Monitoring/Conditional Variable Filters/
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 with the category behavior of /Authentication/Verify and category outcome of Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/
Network Login Events	This filter identifies events with the category behavior of /Authentication/Verify and category device group starting with Network.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Network/
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Foundation/Configuration Monitoring/Detail/Configuration Changes/Device/Database/
Successful Windows Login	This filter detects successful Windows login events (Device Event Class ID = Security:528). The filter looks for the following types of logins: console (2), lock (7), and remote (10).	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Operating System/
Firewall Login Events	This filter identifies firewall events with the category behavior of /Authentication/Verify.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/
Successful VPN Login Events	This filter identifies VPN events with the category behavior of /Authentication/Verify and category outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/
Failed VPN Login Events	This filter identifies VPN events with the category behavior of /Authentication/Verify and category outcome of Failure.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/

Resource	Description	Type	URI
Failed Identity Management Login Attempts	This filter identifies events where an authentication attempt failed.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Identity Management/
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/
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 with the category device group of Operating System.	Filter	ArcSight Foundation/Common/Device Class Filters/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	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 with the category behavior of /Authentication/Verify and category outcome of Success.	Filter	ArcSight Foundation/Intrusion Monitoring/User Tracking/Firewall/
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 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/
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/

Resource	Description	Type	URI
Top Hosts by Number of Connections	This report shows a summary of the number of firewall 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/Firewall/
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/
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/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall 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/Firewall/
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/
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/
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/

Resource	Description	Type	URI
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 database login events in a table sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Database/
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/
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/
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/
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 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/

Resource	Description	Type	URI
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/
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 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/
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/
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/
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/

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 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 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 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/
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/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall 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/Firewall/
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/

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 database login events in a table sorted chronologically.	Focused Report	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Database/
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 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 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 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/
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/

Resource	Description	Type	URI
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/
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/
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/
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 successes 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/

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 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/
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 identifies VPN events where 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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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.

Devices

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

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

Configuration

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. This data is used by the Top 10 Reconnaissance Types Detected trend.
 - ◆ **Top 10 Reconnaissance Types Detected**—This trend collects the top 10 reconnaissance event types per day from the Reconnaissance Types Detected trend. This data is used by the Reconnaissance Types Detected Trend report.

Resources

The following table lists all the resources in the Reconnaissance resource group and any dependant resources.

Table 3-9 Resources that Support the Reconnaissance Group

Resource	Description	Type	URI
Monitor Resources			
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/
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/
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/

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 does not show any results until these trends have been enabled and have become sufficiently populated.	Report	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Reconnaissance/
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/
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/

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/

Library - Correlation Resources

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/
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/

Resource	Description	Type	URI
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/
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/
Library Resources			
Hostile List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Suspicious List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers
Untrusted List	This resource has no description.	Active List	ArcSight System/Attackers
Reconnaissance List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Scanned List	This resource has no description.	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
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/

Resource	Description	Type	URI
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/
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 resource has no description.	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/
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 resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	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/

Resource	Description	Type	URI
Reconnaissance Events (Internal Targets)	This filter identifies events that match the .../Boundary Filters/Internal Target, .../Event Types/Not Correlated and Not Closed and Not Hidden, and .../Event Types/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 resource has no description.	Filter	ArcSight System/Event Types
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/
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/

Resource	Description	Type	URI
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/
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/
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/

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/
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/
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/

Resource	Description	Type	URI
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/
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/
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/
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/

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/
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/
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.

Devices

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

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

Configuration

The Regulated Systems resource group requires the following configuration for your environment:

- 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 13](#).

Resources

The following table lists all the resources in the Regulated Systems resource group and any dependant resources.

Table 3-10 Resources that Support the Regulated Systems Group

Resource	Description	Type	URI
Monitor Resources			
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/

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/
Library Resources			
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	Filter that 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/
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/

Resource	Description	Type	URI
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/

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.

Devices

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

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

Configuration

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.

Resources

The following table lists all the resources in the Resource Access resource group and any dependant resources.

Table 3-11 Resources that Support the Resource Access Group

Resource	Description	Type	URI
Monitor Resources			
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
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/
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/

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/
Library - Correlation Resources			
Resource Access Initiation	This rule detects resource access initiation events as defined by the Access Initiation Events filter and terminates the sessions in the Resource Access session list. The rule also sets the categoryDeviceGroup field to Security Information Manager and the categorySignificance to Informational.	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. The rule also sets the categoryDeviceGroup field to Security Information Manager and the categorySignificance to Informational.	Rule	ArcSight Foundation/Intrusion Monitoring/Resource Access/

Resource	Description	Type	URI
Brute Force Resource Access Initiation	This rule detects brute force resource access initiation events (defined by the Access Initiation Events filter) and terminates the sessions in the Resource Access session list. The rule also sets the categoryDeviceGroup field to Security Information Manager and the categorySignificance to Informational.	Rule	ArcSight Foundation/Intrusion Monitoring/Resource Access/
Library Resources			
Worm Infected Systems	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers
Resource Access	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 * 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	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/
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	Filter that matches all events.	Filter	ArcSight System/Core

Resource	Description	Type	URI
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 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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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/
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/

Resource	Description	Type	URI
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.

Devices

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

Resources

The following table lists all the resources in the Revenue Generating Systems resource group and any dependant resources.

Table 3-12 Resources that Support the Revenue Generating Systems Group

Resource	Description	Type	URI
Monitor Resources			
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/

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/
Library Resources			
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	Filter that matches all events.	Filter	ArcSight System/Core

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/
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/

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.

Devices

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

Resources

The following table lists all the resources in the SANS Top 5 Reports resource group and any dependant resources.

Table 3-13 Resources that Support the SANS Top 5 Reports Group

Resource	Description	Type	URI
Monitor Resources			
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/
Top 10 Vulnerable Systems - Today	This report shows the top ten current vulnerable systems.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/
Top 5 IDS Signatures per Day	This report shows the Top five IDS signatures per day. You can focus this report by device vendor and product.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 5 Users with Failed Logins - Today	This report shows the top five users with the biggest number of failed logins attempts.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/

Resource	Description	Type	URI
Total Number of Vulnerable Systems - Yearly	This report shows the total number of vulnerable systems by week for a given year.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Trend Reports/
Total Number of Vulnerable Systems - Monthly	This report shows the total number of vulnerable systems by week for a given month.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Trend Reports/
Top 5 IDS Signature Destinations per Day	This report shows the top five IDS signature destinations per day.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Top 5 IDS Signature Sources per Day	This report shows the Top five IDS signature sources per day.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Number of Failed Logins - Weekly	This report shows the number of failed logins per day for a given week.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Trend Reports/
Vulnerability Scanner Logs - by Host	This report shows vulnerability scanner logs grouped by zone and host IP address. You can focus this report by device vendor and device product. The report defaults to the McAfee FoundScan device.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/
Top 10 Talkers	This report shows the Top ten talkers and a detailed list of the top talkers.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Number of Failed Logins - Daily	This report shows the number of failed logins per hour for a given day.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Trend Reports/

Resource	Description	Type	URI
Top 5 Users with Failed Logins - Weekly	This report shows the top five users with the biggest number of failed login attempts for a given week.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Trend Reports/
Top Target IPs	This report shows the top ten target IP addresses with a detailed list of the top targets.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/
Vulnerability Scanner Logs - by Vulnerability	This report shows vulnerability scanner logs grouped by vulnerability IDs and names. You can focus this report by device vendor and device product. The report defaults to the McAfee FoundScan device.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/
Top 5 Users with Failed Logins - Daily	This report shows the top five users with the biggest number of failed login attempts for a given day.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Trend Reports/
Number of Failed Logins - Today	This report shows the number of failed logins per hour for the last day.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/
Top 10 Vulnerable Systems - Weekly	This report shows the top ten vulnerable systems for a given week.	Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Trend Reports/
Library Resources			
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/

Resource	Description	Type	URI
Scanner Events	This filter identifies events from network vulnerability scanners, where the events are defined as: Category Behavior = /Found/Vulnerable Category Device Group = /Assessment Tools Category Technique StartsWith /Scan Category Technique Contains vulnerability This filter is used by the Vulnerability Scanner Events active channel.	Filter	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
All Events	Filter that matches all events.	Filter	ArcSight System/Core
Top 5 IDS Signatures per Day (Snort-Snort)	This report shows the top five Snort signatures per day in a chart.	Focused Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Focused Reports/
Top 5 Signatures per Day (CISCO-CiscoSecureIDS)	This report shows the top five Cisco Secure IDS signatures per day in a chart.	Focused Report	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Focused Reports/
Top Users with Failed Logins per Day	This query returns the day, the target user name, and the number of occurrences for failed authentication verifications.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Top Users with Failed Logins/Event Queries/
Failed Logins per Hour	This query returns the hour and the number of occurrences for failed authentication verifications.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Number of Failed Logins/Event Queries/
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/

Resource	Description	Type	URI
Failed Logins per Hour	This query returns the hour and the number of occurrences for failed authentication verifications.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Number of Failed Logins/Event Queries/
Top Users with Failed Logins per Week	This query on the Top Users with Failed Logins per Day trend returns the sum of the number of failed logins for each username within the week.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Top Users with Failed Logins/Trend Queries/
Top IDS Signatures by IDS Product	This query on base /IDS/Network events for the device product and vendor Snort, returns the device event class ID and the count based on the end time. Snort is the default setting. You can select a different device vendor when running the report.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 5 IDS Signatures per Day/
Top Vulnerable Systems per Week	This query on the Number of Vulnerabilities per Asset trend returns the asset name, IP address, host name, and device zone name and averages the number of vulnerabilities associated with that device per week.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Top Vulnerable Systems/Trend Queries/
Top IDS Signature Sources per Day	This query over base IDS/Network events returns the attacker address, attacker zone name, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 5 IDS Signature Sources per Day/
Top 10 Talkers	This query returns the attacker zone name, attacker address ,and the count of events in which 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 event name.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 10 Talkers/
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/

Resource	Description	Type	URI
Number of Vulnerabilities per Asset	This query on assets returns the asset name, IP address, host name, and device zone name and counts the number of vulnerabilities associated with that device.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Top Vulnerable Systems/Asset Queries/
Top IDS Signature Destinations per Day	This query over base IDS/Network events returns the target address, target zone name, device vendor, device product, and the count of the events within the query timeframe.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/5 - Suspicious or Unauthorized Network Traffic Patterns/Top 5 IDS Signature Destinations per Day/
Number of Vulnerabilities per Week	This query on the Number of Vulnerabilities per Asset trend returns the asset name, IP address, host name, and device zone name and averages the number of vulnerabilities associated with that device per week.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Total Number of Vulnerable Systems/Trend Queries/
Failed Logins per Day	This query on the Top Users with Failed Logins per Hour trend returns the sum of the number of failed logins for the day.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Number of Failed Logins/Trend Queries/
Vulnerability Scanner Logs	This query retrieves events for scanner events (defaulting to the McAfee FoundScan scanner) and returns the target address, the target zone name, the device event class ID, and the event (vulnerability) name.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/Vulnerability Scanner Logs - by Host/
Top Users with Failed Logins per Day	This query returns the day, the target user name, and the number of occurrences for failed authentication verifications.	Query	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/Top Users with Failed Logins/Event Queries/
Top Users with Failed Logins per Day	This trend stores the top 1000 users with the highest number of failed logins per day.	Trend	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/

Resource	Description	Type	URI
Number of Vulnerabilities per Asset	This trend stores the number of vulnerabilities associated to an asset on a weekly basis.	Trend	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/4 - Systems Most Vulnerable to Attack/
Failed Logins per Hour	This trend stores the number of failed logins per hour and is scheduled for a daily run.	Trend	ArcSight Foundation/Intrusion Monitoring/SANS Top 5 Reports/1 - Attempts to Gain Access Through Existing Accounts/

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.

Devices

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

Configuration

The Sans Top 20 resource group requires the following configuration for your environment:

- ◆ 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.

Resources

The following table lists all the resources in the Sans Top 20 resource group and any dependant resources.

Table 3-14 Resources that Support the SANS Top 20 Group

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

Resource	Description	Type	URI
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/

Library - Correlation Resources

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 http://www.sans.org/top20/2005/#w1) 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. 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 Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft Task Scheduler Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-022 and CVE:CAN-2004-0212.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) 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. 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 WINS Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft WINS Vulnerability Exploited Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-045, CVE:CAN-2004-0567 and CVE:CAN-2004-1080</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) 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. 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 SMB Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft SMB Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name 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>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w4 for details). 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. 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. If the above conditions are met, the following actions are taken: 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 agentSeverity = Medium categoryBehavior = /Communicate/Query categoryObject = /Host/Operating System, categoryOutcome = /Attempt categorySignificance = /Compromise categoryTechnique = /Exploit/Vulnerability deviceCustomString1Label = Rule Type deviceCustomString1 = SANS Top 20 (v6.01) deviceCustomString2Label = Vulnerability Area deviceCustomString2 = Email deviceCustomString3Label = Vulnerability Name deviceCustomString3 = Microsoft Office XP buffer overflow vulnerability Exploit Attempt The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-005 and CVE:CAN-2004-0848.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Email/

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 http://www.sans.org/top20/2005/#w1) for the Microsoft Plug and Play Service vulnerability. The Microsoft Plug and Play Service contains buffer overflows that might allow a remote user to execute arbitrary code. 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. 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 Plug and Play Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft Plug and Play Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name 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>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) for the Microsoft NetDDE Service vulnerability. 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. 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. 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 NetDDE Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft NetDDE Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-031 and CVE:CAN-2004-0206.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) 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. 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 NNTP Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft NNTP Service Vulnerabilities Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS04-036 and CVE:CAN-2004-0574.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) for the Microsoft License Logging Service vulnerabilities. The Microsoft License Logging service has an unchecked buffer that might allow an attacker to remotely execute arbitrary code. 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. 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 License Logging Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft License Logging Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-010 and CVE:CAN-2005-0050.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1 for details) for the Exchange SMTP Service vulnerability. 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. 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. 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. 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 Exchange SMTP Service Vulnerability Exploited agentSeverity: Very High categoryBehavior: /Communicate/Query categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.0.1) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft Exchange SMTP Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-021 and CVE:CAN-2005-0560.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) for the Microsoft MSDTC and COM+ Services vulnerabilities. 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. 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. 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 MSDTC or COM+ Services Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft MSDTC or COM+ Services Vulnerability Exploited Device Custom String3 Label: Vulnerability Name 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>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

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 http://www.sans.org/top20/2005/#w1) for the Microsoft Message Queuing Service vulnerabilities. The Microsoft Message Queuing service has an unchecked buffer that might allow an attacker to remotely execute arbitrary code. 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. 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 Message Queuing Service Vulnerability Exploited agentSeverity: Very-High categoryBehavior: /Execute categoryObject: /Host/Operating System categoryOutcome: /Success categorySignificance: /Compromise categoryTechnique: /Exploit/Vulnerability Device Custom String1: SANS Top 20 (v6.01) Device Custom String1 Label: Rule Type Device Custom String2: OS Device Custom String2 Label: Vulnerability Area Device Custom String3: Microsoft Message Queuing Service Vulnerability Exploited Device Custom String3 Label: Vulnerability Name. The relevant Microsoft Security Bulletins and CVE identifiers are MSSB:MS05-017 and CVE:CAN-2005-0059.</p>	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/SANS Top 20/Operating Systems/

Resource	Description	Type	URI
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/
Library Resources			
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers
Email	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
Exchange	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type/Email
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 identified 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/

Resource	Description	Type	URI
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
ASM Events	This resource has no description.	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	Filter that 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 identified if an event has an entry for the Target Service Name field.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	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 identified 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/
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/

Resource	Description	Type	URI
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/
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/

Security Overview

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

Devices

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

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

Configuration

The Security Overview resource group requires the following configuration for your environment:

- 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 13](#).

Resources

The following table lists all the resources in the Security Overview resource group and any dependant resources.

Table 3-15 Resources that Support the Security Overview Group

Resource	Description	Type	URI
Monitor Resources			
Intrusion Monitoring - Significant Events	This active channel provides an overview of hostile, compromise, or high priority events. The active channel 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/

Resource	Description	Type	URI
Business Roles	This dashboard displays the status of systems by their business roles: Security Device, Revenue Generation, Infrastructure, Development & Operations and Service. More detailed information is available from the follow-on dashboards in the Detail/Targets groups: Development Assets Infrastructure Assets Operations Assets Revenue Generation Assets Security Device Assets Service Assets This dashboard uses the following data monitors: Status by Security Device Role Status by Infrastructure Role Status by Development and Operations Role Status by Revenue Generation Role Status by Service Role	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/
Executive View	This dashboard provides an overview of the network with respect to attacked systems status by asset location, business role, and worm activity. More detailed information is available from the follow-on dashboards in the Operational Summaries/Executive View Details group: Attacked or Compromised Systems Business Impact by Location Business Impact by Role Business Roles Worm Infected Systems This dashboard uses the following data monitors: Business Impact by Role - Successful Attacks Business Impact by Location - Successful Attacks Status by Business Role Worm Infected Systems	Dashboard	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/

Resource	Description	Type	URI
Worm Infected Systems	This dashboard displays the number of systems infected by worms. More detailed information is available from the follow-on dashboards in the Detail/Attackers/Worm Outbreak group: Worm Outbreak Worm Spread Geo View This dashboard uses the following data monitors: Worm Infected Machines	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	This report displays 4 charts and 6 tables. The first table 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 firing 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.	Report	ArcSight Foundation/Intrusion Monitoring/Executive Summaries/
Library Resources			
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

Resource	Description	Type	URI
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
Infrastructure	This is a site asset category.	Asset Category	Site Asset Categories/Business Impact Analysis/Business Role
Top Attacker IPs	This data monitor collects the counts of attack events and groups them by attacker IP address.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/
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 resource has no description.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Top Connectors	This data monitor provides a list of the top ten ArcSight connectors 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/

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 resource has no description.	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 resource has no description.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
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/Detail/Worm Outbreak/Worm Outbreak/
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 collects the counts of attack events and groups them by the target IP address.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Targets/

Resource	Description	Type	URI
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 resource has no description.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Attacked or Compromised Systems/
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/
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 resource has no description.	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/
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/
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/

Resource	Description	Type	URI
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/
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	This filter retrieves events that have one of the following names: Compromise - Success, Compromise - Attempt, Hostile - Success, Hostile - Attempt. These events are generated by the rules of that name for use in the Attacked or Compromised Systems data monitor.	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 resource has no description.	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	Filter that matches all events.	Filter	ArcSight System/Core
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 resource has no description.	Filter	ArcSight System/Event Types

Resource	Description	Type	URI
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 resource has no description.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
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 resource has no description.	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 resource has no description.	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/

Resource	Description	Type	URI
SIS-Top Attacks Table Query	This query returns the event name and sums the aggregated event count 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/
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/
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 provides information about the state of your environment, such as application and OS status.	Use Case	ArcSight Foundation/Intrusion Monitoring/Security Overview Group/

Resource	Description	Type	URI
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.

Devices

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

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

Resources

The following table lists all the resources in the Targets resource group and any dependant resources.

Table 3-16 Resources that Support the Targets Group

Resource	Description	Type	URI
Monitor Resources			
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/
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/

Resource	Description	Type	URI
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/
Service Attacks	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: Service-Communications Attacks Service-Database Attacks Service-Email Attacks Service-Web Attacks This dashboard uses the Web Service Attack Activity, Email Service Attack Activity, Communications Service Attack Activity, and Database Service Attack Activity data monitors.	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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
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/
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/
Library - Correlation Resources			
Traffic To Dark Address Space	This rule detects any traffic that targets the dark address space and adds the attacker address to the Suspicious active list.	Rule	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
Library Resources			
Hit List	This resource has no description.	Active List	ArcSight System/Targets
Suspicious List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Compromised List	This resource has no description.	Active List	ArcSight System/Threat Tracking

Resource	Description	Type	URI
Compromised User Accounts	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/
Scanned List	This resource has no description.	Active List	ArcSight System/Targets
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 or 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
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

Resource	Description	Type	URI
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/Attackers/
Attacks	This data monitor does not work properly when running in Turbo Mode Fastest.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Attack Monitoring/Attackers/
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/

Resource	Description	Type	URI
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/
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 Assets/Service-Email/
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/
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/

Resource	Description	Type	URI
Very High Criticality Assets	This resource has no description.	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 resource has no description.	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	Filter that 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/
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 resource has no description.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Foundation/Intrusion Monitoring/Attack 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/

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	This filter identifies events in which the priority is greater than 6 and the attacker asset ID is in one of the following groups: /All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Availability Criticality/High /All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Confidentiality Criticality/High /All Asset Categories/Site Asset Categories/Compliance Requirement/FIPS-199/Integrity Criticality/High /All Asset Categories/System Asset Categories/Criticality/High /All Asset Categories/System Asset Categories/Criticality/Very High	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/
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 resource has no description.	Filter	ArcSight System/Event Types
Top 10 Targets	This report shows the top 10 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/

Resource	Description	Type	URI
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/
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/
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/

Resource	Description	Type	URI
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/
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/

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/

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 15](#).

Devices

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

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

Resources

The following table lists all the resources in the Vulnerability View resource group and any dependant resources.

Table 3-17 Resources that Support the Vulnerability View Group

Resource	Description	Type	URI
Monitor Resources			
Vulnerability Events	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. A filter prevents the channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
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/

Resource	Description	Type	URI
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/
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/
Library Resources			

Resource	Description	Type	URI
Vulnerability	This field set shows the following columns: End Time Name Attacker Address Target Address Priority Vulnerability Resource Device Vendor Device Product	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Vulnerability Scanner	This field set shows the following columns: End Time Name Target Zone Resource Target Address Priority Device Vendor Device Product Device Host Name	Field Set	ArcSight Foundation/Intrusion Monitoring/Active Channels/
Scanner Events	This filter identifies events from network vulnerability scanners, where the events are defined as: Category Behavior = /Found/Vulnerable Category Device Group = /Assessment Tools Category Technique StartsWith /Scan Category Technique Contains vulnerability This filter is used by the Vulnerability Scanner Events active channel.	Filter	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
Events with Vulnerabilities	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.	Filter	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
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/

Resource	Description	Type	URI
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/
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/

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/
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/
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/

Resource	Description	Type	URI
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.

Devices

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

Resources

The following table lists all the resources in the Worm Outbreak resource group and any dependant resources.

Table 3-18 Resources that Support the Worm Outbreak Group

Resource	Description	Type	URI
Monitor Resources			
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/

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/

Library - Correlation Resources

Worm Outbreak Detected	This rule is looking for both the Possible Network Sweep rule to trigger and the Target Port Activity by Attacker data monitor to trigger a correlation event that indicates an increase in target port activity by one attacker of more than 100%. Joining the attackers and target ports from these two correlation events determines that the attacker has shown an increase in target port traffic to multiple hosts, not just a two-way communication with a single host. This behavior is indicative of a worm infected system.	Rule	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
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/

Resource	Description	Type	URI
Blaster Infected Host	This rule detects infected hosts by a Blaster worm. This rule looks for 2 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 should 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 will be added in the Worm Infected Systems active list. The correlation event from the rule triggering will be 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/
Library Resources			
Compromised List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Worm Infected Systems	This resource has no description.	Active List	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/
Trusted List	This resource has no description.	Active List	ArcSight System/Attackers
Untrusted List	This resource has no description.	Active List	ArcSight System/Attackers
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type

Resource	Description	Type	URI
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/Detail/Worm Outbreak/Worm Outbreak/
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 resource has no description.	Filter	ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/

Resource	Description	Type	URI
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/
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 resource has no description.	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	Filter that 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 resource has no description.	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/

Appendix A

Upgrading Standard Content

This appendix discusses the following topics.

[“Preparing Existing Content for Upgrade” on page 179](#)

[“Performing the Upgrade” on page 180](#)

[“Checking and Restoring Content After Upgrade” on page 180](#)

Preparing Existing Content for Upgrade

The majority of standard content does not need configuration and does not require special preparation for upgrade. Upgrade preparation is recommended only for content that has been configured and for which configuration is not preserved after the upgrade.

Configurations Preserved During Upgrade

The following resource configurations are preserved during the upgrade process. No restoration is required for these resources after the upgrade.

- Asset modeling for network assets, including:
 - ◆ Assets, and asset groups and their settings
 - ◆ Asset categories applied to assets and asset groups
 - ◆ Vulnerabilities applied to assets
 - ◆ Custom zones
- SmartConnectors
- Users and user groups
- Report schedules
- Notification destinations and priority settings
- Cases

Configurations that Require Restoration After Upgrade

The following resource configurations require restoration after upgrade.

- Any standard content resource that you have modified, including active lists
- Any custom content or special modifications not already described in this document (including customizations performed by ArcSight Professional Services)

Backing Up Existing Resources Before Upgrade



Before you back up existing resources, run the resource validator (`resvalidate.bat`) located on the ESM Manager in `<ARCSIGHT_HOME>\bin\scripts` to check that the resources are working correctly before the upgrade. This prevents you from attributing broken resources with the upgrade.

During the upgrade process, the content is run through a resource validator automatically (see ["Fixing Invalid Resources" on page 181](#)).

To help the process of reconfiguring resources that require restoration after upgrade, back up the resources you identify in ["Configurations that Require Restoration After Upgrade" on page 179](#) and export them in a package. After upgrade, you can re-import the package and use the existing resources as a reference for restoring the configurations to the upgraded environment.

To create a backup of the resources that require restoration after upgrade:

- 1 For each resource type (filter, rule, active list), create a new group under your personal group. Provide a name that identifies the contents.
 - ◆ Right-click your group name and select **New Group**.
- 2 Copy the resources into the new group. Repeat this process for every resource type you want to back up.
 - ◆ Select the resources you want to back up and drag them into the backup folder you created in [Step 1](#). In the *Drag & Drop Options* dialog box, select **Copy**.
- 3 Export the backup groups in a package.
 - ◆ In the Navigator panel Packages tab, right-click your group name and select **New Package**. In the Packages editor in the Inspect/Edit panel, name the package to identify the contents.



Copy and paste configurations from the old resources to the new

Instead of overwriting the new resources with backup copies of the old ones, copy and paste configurations from the old resources one by one into the new ones. This procedure ensures that you preserve your configurations without overwriting any improvements provided in the upgrade.

Performing the Upgrade

After exporting a copy of the configured resources in a backup package, you are ready to perform the upgrade the process. Refer to the ESM upgrade documentation for upgrade procedures.

Checking and Restoring Content After Upgrade

After the upgrade is complete, perform the following checks to verify that all your content has been transferred to the new environment successfully.

Verifying and Reapplying Configurations

Verify and restore standard content after upgrade.

- 1 Verify that your configured resources listed in the section [“Configurations Preserved During Upgrade” on page 179](#) retained their configurations as expected.
- 2 Reconfigure the resources that require restoration.
 - a Re-import the package you created in [“Backing Up Existing Resources Before Upgrade” on page 180](#).
 - b One resource at a time, copy and paste the configurations preserved in the package of copied resources into the new resources installed with the upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old ensures that you retain your configurations without overwriting any improvements provided with the upgraded content.

Verifying Customized Content

It is possible during upgrade that updates to the standard content cause resources you created to work in a way that is not intended. For example, a rule might trigger too often or not at all if it uses a filter in which conditions have been changed.

To verify that the resources you rely upon work as expected, check the following:

- **Trigger events.** Send events that you know trigger the content through the system using the Replay with Rules feature. For more about this feature, refer to the *ArcSight Console User's Guide* or the ESM online Help.
- **Check Live Events.** Check the Live or All Events active channel to verify if the correlation event is triggered. Check that the data monitors you created are returning the expected output based on the test events you send through.
- **Verify notification destinations.** Verify that notifications are sent to the recipients in your notification destinations as expected.
- **Verify active lists.** Check that any active lists you have created to support your content are gathering the replay with rules data as expected.
- **Repair any invalid resources.** During the upgrade process, the resource validator identifies any resources that are rendered invalid (conditions that no longer work) during the upgrade. Find invalid resources and fix their conditions as appropriate. For more about invalid resources, see [Fixing Invalid Resources](#), below.

Fixing Invalid Resources



During the upgrade process, the content is run through a resource validator, which verifies that the values expressed in the resource condition statement still apply to the resource in its new format, and that any resources upon which it depends are still present and also valid. The resource validator runs on any resource that contains a condition statement or populates the asset model, such as:

- Active channels
- Filters
- Data Monitors
- Rules
- Report queries and schedules
- Assets and Asset ranges

- Zones

It is possible that during upgrade, the condition statement for a resource you created or modified becomes invalid. For example, if the schema of an ArcSight-supplied active list changes from one release to another and a resource you created reads entries from this list, the condition statement in the created resource no longer matches the schema of the active list, and the logic is invalid.

When the installer performs the resource validation check and finds an invalid resource, it identifies why the resource is invalid in the report it generates at the end of the upgrade. The upgrade installer also lets you choose to save the reason the resource is invalid in the database (**Persist conflicts to the database=TRUE**). If you choose this option, the upgrade installer:

- Saves the reason the resource is found to be invalid in the database so you can generate a list of invalid resources that you can use later to repair the problems manually.
- Disables the resource so it does not try to evaluate live events in its invalid state.

If you choose not to save the reasons the resource is invalid in the database (**Persist conflicts to the database=FALSE**), the resources remain enabled, which means they try to evaluate the event stream in their invalid state.



If you choose not to persist conflicts to the database and disable invalid resources, the Manager might throw exceptions when the invalid resources try to evaluate live events.

Index

A

- Access Active Sessions query 116
- Access Activity report 111
- Access Attempts by Resource query 117
- Access Closed Sessions query 116
- Access Events by Database Resource report 110
- Access Events by Email Resource report 112
- Access Events by File Resource report 111
- Access Events by Resource report 112
- Access Initiation Events active channel 109
- Access Initiation Events filter 115
- Access Termination Events active channel 110
- Access Termination Events filter 115
- Access to Database Resources filter 114
- Access to Email Resources filter 114
- Access to File Resources filter 114
- ActingUser global variable 82
- active channels
 - Access Initiation Events 109
 - Access Termination Events 110
 - All Access and Authentication Events 110
 - Application Overview 66
 - Business and Data Roles 55
 - Business Roles - Last Hour 54
 - Business Roles - Today 55
 - Data Roles - Last Hour 56
 - Data Roles - Today 56
 - DoS Channel 59
 - Intrusion Monitoring - Significant Events 145
 - Operating System Overview 67
 - Reconnaissance Activity 96
 - Service Overview 66
 - Vulnerability Events 168
 - Vulnerability Scanner Events 168
- active lists
 - Compromised List 48, 159, 176
 - Compromised User Accounts 48, 160
 - Event-based Rule Exclusions 48, 62
 - general configuration 13, 15
 - Hit List 48, 159
 - Hostile List 48, 99
 - Infiltrators List 48
 - Reconnaissance List 99
 - Repetitive Firewall Block List 48
 - Scanned List 99, 160
 - Suspicious List 48, 99, 159
 - Trusted List 48, 61, 99, 114, 142, 176
 - Untrusted List 48, 99, 176
 - User-based Rule Exclusions 48, 79
 - Windows Created Accounts 49, 80
 - Windows Locked Out Accounts 48, 79
 - Windows Login Count 48, 80
 - Worm Infected Systems 114, 176
- Address Spaces asset category 147
- Alert Counts by Device query 21
- Alert Counts by Device report 19
- Alert Counts by Port query 20
- Alert Counts by Port report 19
- Alert Counts by Severity (Chart) query 20
- Alert Counts by Severity query 20
- Alert Counts by Severity report 20
- Alert Counts by Type query 20
- Alert Counts by Type report 20
- Alert Counts per Hour query 21
- Alert Counts per Hour report 19
- Alerts from IDS-IPS resource group 19
- All Access and Authentication Events active channel 110
- All Access and Authentication Events filter 115
- All Events filter 20, 25, 49, 58, 83, 107, 114, 120, 125, 143, 151, 163, 178
- Anti-Virus Activity and Status resource group 22
- Anti-Virus Errors filter 24
- Anti-Virus Errors query 26
- Anti-Virus Events filter 24
- Anti-Virus Overview dashboard 22
- Application Brute Force Logins rule 44
- Application Event Counts data monitor 69
- Application Overview active channel 66
- Application Protocol Event Counts data monitor 149
- Application Protocol is not NULL filter 34, 63, 70, 142
- ArcSight Administration
 - overview 7
- ArcSight Events filter 49, 151, 163
- ArcSight Foundations overview 7
- ArcSight Internal Events filter 57, 64, 70, 85, 100, 143, 152
- ArcSight System
 - overview 7
- ArcSight System Administration asset category 62
- ASM Events filter 58, 64, 70, 83, 101, 143, 151
- asset categories
 - Address Spaces 147
 - ArcSight System Administration 62
 - Business Impact Analysis 57
 - Business Role 57, 99, 147
 - Communications 161
 - Compliance Requirement 107
 - Criticality 160
 - Dark 49, 160
 - Data Role 57, 147
 - Database 160
 - Development 148

- Domain Name Server 177
 - Email 142, 160, 176
 - Exchange 142
 - High 160
 - Infrastructure 148
 - Location 148
 - Microsoft 142, 160
 - North America 160
 - Operating System 68, 142
 - Operations 148
 - Protected 49, 62, 68, 99, 142, 148, 160, 177
 - Proxy 177
 - Revenue Generation 120, 148
 - Role 148
 - Sarbanes-Oxley 107
 - Security Devices 147
 - Service 147
 - Very High 161
 - Vulnerabilities 142
 - Web 160
 - Asset Counts by Vulnerability trend 173
 - Asset Vulnerability List report 169
 - Assets Counts by Vulnerability Trend query 171
 - Attack Counts by Service Query on Trend query 35
 - Attack Counts by Target Zone Query on Trend query 35
 - Attack Events filter 49, 57, 107, 120, 124, 150, 162
 - Attack from Source having Reconnaissance History rule 99
 - Attack From Suspicious Source rule 45
 - Attack Rates by Attacker Zone and Customer data monitor 31
 - Attack Rates by Attacker Zone data monitor 32
 - Attack Rates by Service and Customer data monitor 30
 - Attack Rates by Service and Zones dashboard 28
 - Attack Rates by Service dashboard 29
 - Attack Rates by Service data monitor 30
 - Attack Rates by Targeted Zone and Customer data monitor 32
 - Attack Rates by Targeted Zone data monitor 30
 - Attack Rates by Zones dashboard 27
 - Attack Rates resource group 27
 - Attacked or Compromised Systems dashboard 147
 - Attacked or Compromised Systems data monitor 148
 - Attacked or Compromised Systems filter 151
 - Attacker Counts by ArcSight Priority query 51
 - Attacker Counts by ArcSight Priority report 39
 - Attacker Counts by Attacker Port query 53
 - Attacker Counts by Attacker Port report 38
 - Attacker Counts by Device query 52
 - Attacker Counts by Device report 40
 - Attacker Counts by Target Port query 50
 - Attacker Counts by Target Port report 40
 - Attacker Counts By Target query 52
 - Attacker Counts By Target report 38
 - Attacker Port Counts query 51
 - Attacker Port Counts report 39
 - Attacker User ID is NULL filter 84
 - Attacker User Name and ID are NULL filter 85
 - Attacker User Name is NULL filter 84
 - Attacker Zones by Service and Customer data monitor 30
 - Attacker Zones by Service data monitor 33
 - Attackers resource group 37
 - AttackerUser global variable 82
 - Attacks data monitor 161
 - Attacks Targeting Assets filter 163
 - Authentication Failures by Destination data monitor 81
 - Authentication Failures by Source data monitor 80
 - AV - Failed Updates filter 25
 - AV - Found Infected filter 24
- ## B
- Blaster DDOS From Infected Host rule 175
 - Blaster Infected Host rule 176
 - Bottom 10 Attack Sources query 53
 - Bottom 10 Attackers query 50
 - Bottom 10 Targets query 166
 - Bottom N Attack Sources report 40
 - Bottom N Attackers report 39
 - Bottom N Targets report 158
 - Brute Force Access Active Sessions on Trend query 116
 - Brute Force Access Active Sessions query 116
 - Brute Force Access Activity report 111
 - Brute Force Access Closed Sessions on Trend query 115
 - Brute Force Access Closed Sessions query 117
 - Brute Force Access Session Trends trend 118
 - Brute Force Access Sessions Trend query 116
 - Brute Force Logins rule 41
 - Brute Force Resource Access Initiation rule 114
 - Brute Force Resource Access session list 117
 - Brute Force Session Trends report 110
 - Business and Data Roles active channel 55
 - Business Impact Analysis asset category 57
 - Business Impact Analysis field set 57, 150
 - Business Impact Analysis resource group 54
 - Business Impact Analysis use case 154
 - Business Impact by Location - Successful Attacks data monitor 150
 - Business Impact by Location dashboard 147
 - Business Impact by Role - Successful Attacks data monitor 150
 - Business Impact by Role dashboard 146
 - Business Role - Attempted Attacks query 58
 - Business Role - Attempted Attacks report 57
 - Business Role - Development and Operations filter 151
 - Business Role - Infrastructure filter 152
 - Business Role - Revenue Generation filter 152
 - Business Role - Security Devices filter 152
 - Business Role - Service filter 151
 - Business Role - Successful Attacks query 58
 - Business Role - Successful Attacks report 56
 - Business Role asset category 57, 99, 147
 - Business Roles - Last Hour active channel 54
 - Business Roles - Today active channel 55
 - Business Roles dashboard 146
 - Business Roles Scanned query 102
 - By User Account - Compromised - Access query 165
 - By User Account - Compromised - Access report 158
 - By User Account - Compromised - All Activity query 166
 - By User Account - Compromised - All Activity report 159
- ## C
- Closed Connection Durations query 93
 - Closed VPN Connection Durations query 51
 - Communications asset category 161
 - Communications Service Attack Activity data monitor 162
 - Compliance Requirement asset category 107
 - Compromised List active list 48, 159, 176

Compromised User Accounts active list 48, 160
 configuration
 active lists 13, 15
 Connection Counts by User report 38, 76
 Connection Durations by User report 76
 content packages 8
 Critical Asset (High or Very High) Target Port Not Null filter 164
 Critical Asset Group Count data monitor 161
 Critical Asset Monitoring dashboard 156
 Critical Attacker Assets data monitor 161
 Critical Attacker Assets Priority gt 6 filter 164
 Critical Target Asset filter 163
 Critical Target Asset Priority gt 6 filter 163
 Critical Target Assets data monitor 161
 Critical Target Assets Event Graph data monitor 162
 Critical Target Assets Port Anomalies data monitor 161
 Criticality asset category 160
 Current Environment Status Overview dashboard 67
 Customer Attack Rates by Service and Zones dashboard 28
 Customer Attack Rates by Service dashboard 28
 Customer Attack Rates by Zones dashboard 29

D

Daily Port Scanning Activity on Trend (Chart Query) query 103
 Daily Port Scanning Activity on Trend query 103
 Daily Scanning Events by Business Role on Trend query 104
 Daily Top 10 Resource Access on Trend query 115
 Daily Top 10 Resource Access Trends report 113
 Daily Top 10 Resource Access Trends trend 118
 Daily Top 10 Vulnerabilities in Events Trend report 169
 Dark asset category 49, 160
 dashboards
 Anti-Virus Overview 22
 Attack Rates by Service 29
 Attack Rates by Service and Zones 28
 Attack Rates by Zones 27
 Attacked or Compromised Systems 147
 Business Impact by Location 147
 Business Impact by Role 146
 Business Roles 146
 Critical Asset Monitoring 156
 Current Environment Status Overview 67
 Customer Attack Rates by Service 28
 Customer Attack Rates by Service and Zones 28
 Customer Attack Rates by Zones 29
 Executive View 146
 Firewall Login Overview 75
 Identity Management Overview 75
 Inbound Event Spikes 60
 Network Login Overview 74
 Operating System Login Overview 75
 Reconnaissance Graph 96
 Reconnaissance in Progress 96
 Security Activity Statistics 146
 Service Attacks 156
 Service-Communications Attacks 156
 Service-Database Attacks 155
 Service-Email Attacks 155
 Service-Web Attacks 155
 Successful Inbound Attacks 156

Top 10 Attack Rate Statistics by Service 27
 Top 10 Attack Rate Statistics by Service and Zones 29
 Top 10 Attack Rate Statistics by Zones 28
 Top 10 Customer Attack Rate Statistics by Service 28
 Top 10 Customer Attack Rate Statistics by Service and Zones 28
 Top 10 Customer Attack Rate Statistics by Zones 29
 Virus Activity Overview 22
 Virus Activity Statistics 22
 VPN Login Overview 74
 Worm Infected Systems 147
 Worm Outbreak 174
 Worm Outbreak Overview 174
 Worm Spread Geo View 174
 data monitors
 Application Event Counts 69
 Application Protocol Event Counts 149
 Attack Rates by Attacker Zone 32
 Attack Rates by Attacker Zone and Customer 31
 Attack Rates by Service 30
 Attack Rates by Service and Customer 30
 Attack Rates by Targeted Zone 30
 Attack Rates by Targeted Zone and Customer 32
 Attacked or Compromised Systems 148
 Attacker Zones by Service 33
 Attacker Zones by Service and Customer 30
 Attacks 161
 Authentication Failures by Destination 81
 Authentication Failures by Source 80
 Business Impact by Location - Successful Attacks 150
 Business Impact by Role - Successful Attacks 150
 Communications Service Attack Activity 162
 Critical Asset Group Count 161
 Critical Attacker Assets 161
 Critical Target Assets 161
 Critical Target Assets Event Graph 162
 Critical Target Assets Port Anomalies 161
 Database Service Attack Activity 161
 Email Service Attack Activity 162
 Event Counts by Hour 149
 Events per Address Space 148
 Firewall Accepts 63
 Inbound Event Spikes for Hosts 62
 Inbound Event Spikes for Networks 63
 Inbound Event Spikes for Services 62
 Last 10 Anti-Virus Errors 24
 Last 10 Failed Login Events 80, 81
 Last 10 Hosts Scanned 99
 Last 10 Scanners 100
 Last 10 Successful Login Events 80, 81, 82
 Last 10 Zones Scanned 100
 Login Results 81
 Operating Systems Event Counts 69
 Recent Events 149
 Reconnaissance Graph 100
 Service Event Counts 68
 Status by Business Role 149
 Status by Development and Operations Roles 149
 Status by Infrastructure Role 148
 Status by Revenue Generation Role 150
 Status by Security Device Role 149
 Status by Service Role 150

- Successful Inbound Attacks 150, 162
 - Target Port Activity by Attacker 177
 - Targeted Zones by Service 33
 - Targeted Zones by Service and Customer 31
 - Top 10 Anti-Virus Errors 23
 - Top 10 Application Events 69
 - Top 10 Attacked Services 32
 - Top 10 Attacker Zones 32
 - Top 10 Attacker Zones by Customer 34
 - Top 10 Attacker Zones by Service 31
 - Top 10 Attacker Zones by Service and Customer 33
 - Top 10 Communications Service Targets 162
 - Top 10 Database Service Targets 162
 - Top 10 Email Service Targets 161
 - Top 10 Infected Systems 23
 - Top 10 Infections 23
 - Top 10 Operating System Events 69
 - Top 10 Service Events 69
 - Top 10 Targeted Services by Customer 33
 - Top 10 Targeted Zones 33
 - Top 10 Targeted Zones by Customer 32
 - Top 10 Targeted Zones by Service 31
 - Top 10 Targeted Zones by Service and Customer 31
 - Top 10 Users With Failed Logins 80, 81, 82
 - Top 10 Web Service Targets 162
 - Top 10 Zones Scanned 100
 - Top Attacker IPs 148
 - Top Attackers Targeting Critical Assets 161
 - Top Categories 150
 - Top Connectors 148
 - Top Target IPs 149
 - Top Transport Protocols 150
 - Top Users by Connection Count 81
 - Top Users by Login Activity 80
 - Virus Activity 23
 - Virus Activity by Host 24
 - Virus Activity by Zone 24
 - Web Service Attack Activity 161
 - Worm Activity Status 177
 - Worm Infected Machines 149
 - Worm Infected Systems 149, 177
 - Worm Propagation by Host 177
 - Worm Propagation by Zone 177
 - Worm Spread 177
 - Data Role asset category 57, 147
 - Data Roles - Last Hour active channel 56
 - Data Roles - Today active channel 56
 - Database asset category 160
 - Database Events filter 84
 - Database Resource Access by Users report 111
 - Database Service Attack Activity data monitor 161
 - Denied Inbound Connections by Address query 52
 - Denied Inbound Connections by Address report 39
 - Denied Inbound Connections by Port query 51
 - Denied Inbound Connections by Port report 40
 - Denied Inbound Connections per Hour (Chart) query 53
 - Denied Inbound Connections per Hour query 51
 - Denied Inbound Connections per Hour report 38
 - Denied Outbound Connections by Address query 52
 - Denied Outbound Connections by Address report 39
 - Denied Outbound Connections by Port query 52
 - Denied Outbound Connections by Port report 37
 - Denied Outbound Connections per Hour (Chart) query 53
 - Denied Outbound Connections per Hour report 38
 - Development asset category 148
 - Device SNMP Authentication Failures by User query 93
 - Device SNMP Authentication Failures query 94
 - Device SNMP Authentication Failures report 75
 - Domain Name Server asset category 177
 - DoS Channel active channel 59
 - DoS resource group 59
- ## E
- Email asset category 142, 160, 176
 - Email Resource Access by Users report 111
 - Email Service Attack Activity data monitor 162
 - Environment State resource group 66
 - Environment State use case 153
 - Environment Status Events - Trend query 72
 - Environment Status Events over the Last 24 Hours (Chart Query) query 73
 - Environment Status Events over the Last 24 Hours report 67
 - Environment Status Events trend 73
 - Errors Detected in Anti-Virus Deployment report 23
 - Event Counts by Hour data monitor 149
 - Event-based Rule Exclusions active list 48, 62
 - Events for Internal Applications excluding services filter 70
 - Events for Internal Operating Systems filter 71
 - Events for Internal Services filter 70
 - Events per Address Space data monitor 148
 - Events with Vulnerabilities filter 170
 - Exchange asset category 142
 - Executive View dashboard 146
 - External Source filter 49, 151, 162
 - External Target filter 50, 143, 178
- ## F
- Failed Anti-Virus Updates Chart query 25
 - Failed Anti-Virus Updates query 25
 - Failed Anti-Virus Updates report 23
 - Failed Firewall Login Events filter 84
 - Failed Identity Management Login Attempts filter 85
 - Failed Login Attempts (Chart) query 93
 - Failed Login Attempts focused report 85, 87
 - Failed Login Attempts query 92
 - Failed Login Attempts report 75
 - Failed Login by User (Chart) query 92
 - Failed Login by User query 92
 - Failed Login Events filter 83
 - Failed Logins by Destination Address (Chart) query 91
 - Failed Logins by Destination Address focused report 86, 87, 88, 91
 - Failed Logins by Destination Address report 76
 - Failed Logins by Source Address (Chart) query 93
 - Failed Logins by Source Address focused report 85, 89, 90, 91
 - Failed Logins by Source Address report 77
 - Failed Logins by Source-Destination Pair query 93
 - Failed Logins by User focused report 86, 88, 89, 90, 91
 - Failed Logins by User report 76
 - Failed Logins per Day query 127
 - Failed Logins per Hour query 125, 126
 - Failed Logins per Hour trend 128
 - Failed Network Login Events filter 83

- Failed Operating System Login Events filter 83
- Failed VPN Login Events filter 84
- field sets
 - Business Impact Analysis 57, 150
 - Resource Access 114
 - Status Overview 69
 - Vulnerability 170
 - Vulnerability Scanner 170
- File Resource Access by Users report 112
- filters
 - Access Initiation Events 115
 - Access Termination Events 115
 - Access to Database Resources 114
 - Access to Email Resources 114
 - Access to File Resources 114
 - All Access and Authentication Events 115
 - All Events 20, 25, 49, 58, 83, 107, 114, 120, 125, 143, 151, 163, 178
 - Anti-Virus Errors 24
 - Anti-Virus Events 24
 - Application Protocol is not NULL 34, 63, 70, 142
 - ArcSight Events 49, 151, 163
 - ArcSight Internal Events 57, 64, 70, 85, 100, 143, 152
 - ASM Events 58, 64, 70, 83, 101, 143, 151
 - Attack Events 49, 57, 107, 120, 124, 150, 162
 - Attacked or Compromised Systems 151
 - Attacker User ID is NULL 84
 - Attacker User Name and ID are NULL 85
 - Attacker User Name is NULL 84
 - Attacks Targeting Assets 163
 - AV - Failed Updates 25
 - AV - Found Infected 24
 - Business Role - Development and Operations 151
 - Business Role - Infrastructure 152
 - Business Role - Revenue Generation 152
 - Business Role - Security Devices 152
 - Business Role - Service 151
 - Critical Asset (High or Very High) Target Port Not Null 164
 - Critical Attacker Assets Priority gt 6 164
 - Critical Target Asset 163
 - Critical Target Asset Priority gt 6 163
 - Database Events 84
 - Events for Internal Applications excluding services 70
 - Events for Internal Operating Systems 71
 - Events for Internal Services 70
 - Events with Vulnerabilities 170
 - External Source 49, 151, 162
 - External Target 50, 143, 178
 - Failed Firewall Login Events 84
 - Failed Identity Management Login Attempts 85
 - Failed Login Events 83
 - Failed Network Login Events 83
 - Failed Operating System Login Events 83
 - Failed VPN Login Events 84
 - Firewall Accepts 63
 - Firewall Events 65, 84
 - Firewall Login Events 84
 - High Criticality Assets 163
 - Identity Management Connection Start Events 82
 - Identity Management Events 85
 - IDS -IPS Events 20, 49, 64, 124, 163
 - Inbound Attacks 151, 163
 - Inbound Events 50, 152, 163
 - Inbound Events for Hosts 64
 - Inbound Events for Networks 64
 - Inbound Events for Service 63
 - Internal Source 49, 143, 151, 163, 178
 - Internal Target 49, 64, 70, 101, 143, 151, 163, 178
 - Internal to Internal Events 178
 - LockedCount is NULL 83
 - Login Events 82
 - LoginCount is NULL or 0 84
 - Network Events 82
 - Network Login Events 84
 - Non-ArcSight Events 50, 152, 164
 - Non-ArcSight Internal Events 57, 64, 70, 85, 100, 143, 152
 - Not Correlated and Not Closed and Not Hidden 100
 - Operating System Events 85
 - Operating System Login Events 83
 - Outbound Events 49, 178
 - Possible Attack Events 34, 63
 - Reconnaissance Events (Internal Targets) 101
 - Reconnaissance Events by Attacker 100
 - Reconnaissance Events by Target 100
 - Reconnaissance Events by Target Zone 100
 - Scanner Events 125, 170
 - Services - Communications Service 164
 - Services - Database Service 163
 - Services - Email Service 164
 - Services - Web Service 162
 - Status by Business Role 151
 - Successful Attacks 58, 152
 - Successful Firewall Login Events 85
 - Successful Inbound DoS Events - Trend Filter 64, 142
 - Successful Login Events 83
 - Successful Network Login Events 83
 - Successful Operating System Login Events 83
 - Successful VPN Login Events 84
 - Successful Windows Login 49, 84
 - Successful Windows Logout 82
 - Target Address is NULL 24
 - Target Asset has Asset Name 64, 70, 143
 - Target Asset has OS Categorization 70
 - Target Host Name is NULL 24
 - Target Object starts with Host Application 70
 - Target Port Activity By Attacker 177
 - Target Port is not NULL 34, 64, 70, 142
 - Target Service Name is not NULL 34, 64, 70, 143
 - Target User ID is NULL 49, 83
 - Target User Name is NULL 85
 - Target Zone is NULL 25
 - Targeted Business Impact Analysis 57
 - Transport Protocol is not NULL 34, 65, 71, 143
 - Update Events 25
 - Very High Criticality Assets 163
 - Virus Activity 24
 - VPN Events 82
 - VPN Login Events 83
 - Worm Activity 178
 - Worm Geo Filter 178
 - Worm Infected Systems 178
 - Worm Outbreak 150, 177
 - Worm Traffic 152, 178
 - Firewall - Application Protocol Scan rule 98

- Firewall - High Volume Accepts rule 44
- Firewall - Host Port Scan rule 98
- Firewall - Network Port Scan rule 99
- Firewall - Pass After Repetitive Blocks rule 42
- Firewall - Repetitive Block - In Progress rule 42
- Firewall Accepts data monitor 63
- Firewall Accepts filter 63
- Firewall Events filter 65, 84
- Firewall Login Events filter 84
- Firewall Login Overview dashboard 75
- focused reports
 - Failed Login Attempts 85, 87
 - Failed Logins by Destination Address 86, 87, 88, 91
 - Failed Logins by Source Address 85, 89, 90, 91
 - Failed Logins by User 86, 88, 89, 90, 91
 - Login Event Audit 87, 89, 90
 - Successful Logins by Destination Address 87, 88
 - Successful Logins by Source Address 85, 86, 89, 90
 - Successful Logins by User 86, 87, 88, 90
 - Top 10 Alerts 20
 - Top 10 Attackers 50
 - Top 10 Targets 164
 - Top 5 IDS Signatures per Day (Snort-Snort) 125
 - Top 5 Signatures per Day (CISCO-CiscoSecureIDS) 125
 - Top Hosts by Number of Connections 86, 89

G

- global variables
 - ActingUser 82
 - AttackerUser 82
 - TargetUser 82

H

- High asset category 160
- High Criticality Assets filter 163
- High Number of IDS Alerts for Backdoor rule 42
- High Number of IDS Alerts for DoS rule 61
- Hit List active list 48, 159
- Hostile List active list 48, 99

I

- Identity Management Connection Start Events filter 82
- Identity Management Events filter 85
- Identity Management Overview dashboard 75
- IDS -IPS Events filter 20, 49, 64, 124, 163
- Inbound Attacks filter 151, 163
- Inbound DoS Events - Yesterday report 60
- Inbound DoS Events trend 65, 144
- Inbound Event Spikes dashboard 60
- Inbound Event Spikes for Hosts data monitor 62
- Inbound Event Spikes for Networks data monitor 63
- Inbound Event Spikes for Services data monitor 62
- Inbound Events filter 50, 152, 163
- Inbound Events for Hosts filter 64
- Inbound Events for Networks filter 64
- Inbound Events for Service filter 63
- Infected Systems query 25
- Infiltrators List active list 48
- Infrastructure asset category 148
- Internal Source filter 49, 143, 151, 163, 178

- Internal Target filter 49, 64, 70, 101, 143, 151, 163, 178
- Internal to Internal Events filter 178
- Intrusion Monitoring - Significant Events active channel 145
- invalid resources 181

L

- Last 10 Anti-Virus Errors data monitor 24
- Last 10 Failed Login Events data monitor 80, 81
- Last 10 Hosts Scanned data monitor 99
- Last 10 Scanners data monitor 100
- Last 10 Successful Login Events data monitor 80, 81, 82
- Last 10 Zones Scanned data monitor 100
- Location asset category 148
- LockedCount is NULL filter 83
- Login Errors by User (Chart) query 93
- Login Errors by User query 92
- Login Errors by User report 77
- Login Event Audit focused report 87, 89, 90
- Login Event Audit query 91
- Login Event Audit report 75
- Login Events filter 82
- Login Results data monitor 81
- Login Tracking resource group 74
- LoginCount is NULL or 0 filter 84

M

- Microsoft asset category 142, 160
- Multi Host Application Brute Force Logins rule 43
- Multiple Login Attempts to Locked Windows Account rule 44
- Multiple Windows Logins by Same User rule 47

N

- Network Events filter 82
- Network Login Events filter 84
- Network Login Overview dashboard 74
- Non-ArcSight Events filter 50, 152, 164
- Non-ArcSight Internal Events filter 57, 64, 70, 85, 100, 143, 152
- North America asset category 160
- Not Correlated and Not Closed and Not Hidden filter 100
- Notify on Successful Attack rule 44
- Number of Failed Logins - Daily report 123
- Number of Failed Logins - Today report 124
- Number of Failed Logins - Weekly report 123
- Number of Vulnerabilities per Asset query 127
- Number of Vulnerabilities per Asset trend 128
- Number of Vulnerabilities per Week query 127

O

- Operating System asset category 68, 142
- Operating System Events filter 85
- Operating System Login Events filter 83
- Operating System Login Overview dashboard 75
- Operating System Overview active channel 67
- Operating Systems Event Counts data monitor 69
- Operations asset category 148
- Outbound Events filter 49, 178

P

packages

- deleting 12
- installing 11
- uninstalling 11

Port Scanning Activity report 98

Port Scanning Activity Trend report 96

Port Scanning Daily Top 20 trend 104

Port Scanning Daily Top 20, Trend on Trend query 102

Port Scanning trend 105

Port Scanning Trend query 102

Ports Scanned query 102

Possible Attack Events filter 34, 63

Possible DoS on Hosts rule 60

Possible DoS on Network rule 61

Possible DoS on Services rule 61

Possible Internal Network Sweep rule 176

Possible Outbound Network Sweep rule 176

Prioritized Attack Counts by Service - Last 24 Hours report 29

Prioritized Attack Counts by Service - Last Hour query 34

Prioritized Attack Counts by Service - Trend query 36

Prioritized Attack Counts by Service Query on Trend query 34

Prioritized Attack Counts by Service trend 36

Prioritized Attack Counts by Target Zone - Last 24 Hours report 29

Prioritized Attack Counts by Target Zone - Last Hour query 35

Prioritized Attack Counts by Target Zone - Trend query 35

Prioritized Attack Counts by Target Zone Query on Trend query 35

Prioritized Attack Counts by Target Zone trend 36

Prioritized Scanning Activity by Business Role report 97

Prioritized Scanning Activity by Zone report 97

Prioritized Vulnerabilities in Events by Zone query 171

Prioritized Vulnerability Events by Zone trend 172

Probable Attack - Script Attack rule 47

Probable Successful Attack - Brute Force rule 47

Probable Successful Attack - DoS rule 43

Probable Successful Attack - Execute rule 46

Probable Successful Attack - Exploit rule 42

Probable Successful Attack - Information Leak rule 46

Probable Successful Attack - Probable Redirect Attack rule 45

Probable Successful Attack - Repetitive Exploit Events rule 40

Probable Successful Attack - System Configuration rule 41

Protected asset category 49, 62, 68, 99, 142, 148, 160, 177

Proxy asset category 177

Q

queries

Access Active Sessions 116

Access Attempts by Resource 117

Access Closed Sessions 116

Alert Counts by Device 21

Alert Counts by Port 20

Alert Counts by Severity 20

Alert Counts by Severity (Chart) 20

Alert Counts by Type 20

Alert Counts per Hour 21

Anti-Virus Errors 26

Assets Counts by Vulnerability Trend 171

Attack Counts by Service Query on Trend 35

Attack Counts by Target Zone Query on Trend 35

Attacker Counts by ArcSight Priority 51

Attacker Counts by Attacker Port 53

Attacker Counts by Device 52

Attacker Counts By Target 52

Attacker Counts by Target Port 50

Attacker Port Counts 51

Bottom 10 Attack Sources 53

Bottom 10 Attackers 50

Bottom 10 Targets 166

Brute Force Access Active Sessions 116

Brute Force Access Active Sessions on Trend 116

Brute Force Access Closed Sessions 117

Brute Force Access Closed Sessions on Trend 115

Brute Force Access Sessions Trend 116

Business Role - Attempted Attacks 58

Business Role - Successful Attacks 58

Business Roles Scanned 102

By User Account - Compromised - Access 165

By User Account - Compromised - All Activity 166

Closed Connection Durations 93

Closed VPN Connection Durations 51

Daily Port Scanning Activity on Trend 103

Daily Port Scanning Activity on Trend (Chart Query) 103

Daily Scanning Events by Business Role on Trend 104

Daily Top 10 Resource Access on Trend 115

Denied Inbound Connections by Address 52

Denied Inbound Connections by Port 51

Denied Inbound Connections per Hour 51

Denied Inbound Connections per Hour (Chart) 53

Denied Outbound Connections by Address 52

Denied Outbound Connections by Port 52

Denied Outbound Connections per Hour 52

Denied Outbound Connections per Hour (Chart) 53

Device SNMP Authentication Failures 94

Device SNMP Authentication Failures by User 93

Environment Status Events - Trend 72

Environment Status Events over the Last 24 Hours (Chart Query) 73

Failed Anti-Virus Updates 25

Failed Anti-Virus Updates Chart 25

Failed Login Attempts 92

Failed Login Attempts (Chart) 93

Failed Login by User 92

Failed Login by User (Chart) 92

Failed Logins by Destination Address (Chart) 91

Failed Logins by Source Address (Chart) 93

Failed Logins by Source-Destination Pair 93

Failed Logins per Day 127

Failed Logins per Hour 125, 126

Infected Systems 25

Login Errors by User 92

Login Errors by User (Chart) 93

Login Event Audit 91

Number of Vulnerabilities per Asset 127

Number of Vulnerabilities per Week 127

Port Scanning Daily Top 20, Trend on Trend 102

Port Scanning Trend 102

- Ports Scanned 102
- Prioritized Attack Counts by Service - Last Hour 34
- Prioritized Attack Counts by Service - Trend 36
- Prioritized Attack Counts by Service Query on Trend 34
- Prioritized Attack Counts by Target Zone - Last Hour 35
- Prioritized Attack Counts by Target Zone - Trend 35
- Prioritized Attack Counts by Target Zone Query on Trend 35
- Prioritized Vulnerabilities in Events by Zone 171
- Recent Activity Affecting Target Assets in Compromised List 166
- Recent Activity Affecting Target Assets in Hit List 167
- Recent Activity Affecting Target Assets in Scanned List 166
- Reconnaissance Activity Trend 103
- Reconnaissance Types Detected 102
- Reconnaissance Types Detected on Trend 101
- Reconnaissance Types Detected on Trend (Chart Query) 103
- Reconnaissance Types Detected Trend 104
- Regulated Systems - By Attack 107
- Regulated Systems - By Host - Attacked 108
- Regulated Systems - Count Vulnerabilities 108
- Resource Access Attempts 116
- Resource Access on Trend 116
- Resource Access Trend 117
- Resource Accesses 115
- Revenue Generating Systems - Attacked 121
- Revenue Generating Systems - Compromise - All 121
- Revenue Generating Systems - Compromise - Availability 121
- Revenue Generating Systems - Compromise - Confidentiality 121
- Revenue Generating Systems - Compromise - Integrity 121
- SANS Top 20 (v6.01) Attacked Systems - hourly 143
- Sarbanes-Oxley - Top 10 Targets 107
- SIS-Assets Compromised Table Query 153
- SIS-Cases Added Table Query 153
- SIS-Event Count by Agent Severity Chart Query 152
- SIS-Notifications Sent Table Query 153
- SIS-Top Attackers Chart Query 153
- SIS-Top Attacks Table Query 153
- SIS-Top Events Table Query 153
- SIS-Top Firing Rules Table Query 152
- SIS-Top Target Ports Chart Query 153
- SIS-Top Targets Chart Query 153
- SNMP Authentication Failures by Device 93
- Successful Inbound DoS Events - Trend 65, 144
- Successful Inbound DoS Events Last Hour 65
- Successful Inbound DoS Events Query on Trend 65, 143
- Successful Login by User 92
- Successful Login by User (Chart) 94
- Successful Logins by Destination Address (Chart) 93
- Successful Logins by Source Address (Chart) 91
- Successful Logins by Source-Destination Pair 94
- Target Counts by ArcSight Priority 165
- Target Counts by Attacker 166
- Target Counts by Attacker Port 52
- Target Counts by Device 167
- Target Counts by Event Name 167
- Target Counts by Target Port 166
- Target Port Counts 166
- Targets in Compromised List 166
- Targets in Hit List 165
- Targets in Scanned List 164
- Top 10 Attack Signatures targeting Windows Assets 165
- Top 10 Attack Sources 51
- Top 10 Attacked Assets in North America 165
- Top 10 Attacker Details 51
- Top 10 Attackers 50
- Top 10 Daily Vulnerabilities in Events on Trend 171
- Top 10 Daily Vulnerability Events on Trend 172
- Top 10 Reconnaissance Types Detected on Trend 101
- Top 10 Talkers 126
- Top 10 Targets 125, 165
- Top Alert Destinations 165
- Top Alert Sources 50
- Top Anti-Virus Errors 26
- Top Application Status Events on Trend 71
- Top Application Status Events over the Last 24 Hours 72
- Top Application Status Events over the Last 24 Hours (Chart Query) 73
- Top Attacker Ports 50
- Top Connection Durations 92
- Top Hosts by Number of Connections 93
- Top IDS and IPS Alerts 20, 126
- Top IDS Signature Destinations per Day 127
- Top IDS Signature Sources per Day 126
- Top IDS Signatures by IDS Product 126
- Top Infected Systems 26
- Top N Vulnerabilities in Events on Trend 171
- Top Operating System Status Events on Trend 72
- Top OS Status Events over the Last 24 Hours 71
- Top OS Status Events over the Last 24 Hours (Chart Query) 73
- Top Service Status Events on Trend 71
- Top Service Status Events over the Last 24 Hours 72
- Top Service Status Events over the Last 24 Hours (Chart Query) 71
- Top Status Events on Trend 71
- Top Target Ports Chart 167
- Top Users by Connection Count 53, 92
- Top Users with Failed Logins per Day 125, 127
- Top Users with Failed Logins per Week 126
- Top VPN Connection Durations 52
- Top Vulnerable Systems per Week 126
- Top Zones with Anti-Virus Errors 25
- Update Summary 26
- Update Summary Chart 26
- User Activity 91
- Users by Connection Count 52, 92
- Users with Open Connections 91
- Users with Open VPN Connections 53
- Virus Activity by Hour 25
- Vulnerabilities (by Asset Counts) on Trend 171
- Vulnerabilities and Assets 170
- Vulnerabilities in Events by Zone (Chart Query) 170
- Vulnerability Scanner Logs 127
- Windows Events 92

- Worm Infected Systems 178
 - Zone Scanning Activity on Trend 104
 - Zone Scanning Activity on Trend (Chart Query) 104
 - Zone Scanning Events 101
 - Zone Scanning Events by Priority Trend 103
- R**
- Recent Activity Affecting Target Assets in Compromised List query 166
 - Recent Activity Affecting Target Assets in Compromised List report 157
 - Recent Activity Affecting Target Assets in Hit List query 167
 - Recent Activity Affecting Target Assets in Hit List report 159
 - Recent Activity Affecting Target Assets in Scanned List query 166
 - Recent Activity Affecting Target Assets in Scanned List report 156
 - Recent Events data monitor 149
 - Reconnaissance Activity active channel 96
 - Reconnaissance Activity trend 105
 - Reconnaissance Activity Trend query 103
 - Reconnaissance Events (Internal Targets) filter 101
 - Reconnaissance Events by Attacker filter 100
 - Reconnaissance Events by Target filter 100
 - Reconnaissance Events by Target Zone filter 100
 - Reconnaissance Graph dashboard 96
 - Reconnaissance Graph data monitor 100
 - Reconnaissance in Progress dashboard 96
 - Reconnaissance List active list 99
 - Reconnaissance resource group 95
 - Reconnaissance Types Detected by Zone report 98
 - Reconnaissance Types Detected on Trend (Chart Query) query 103
 - Reconnaissance Types Detected on Trend query 101
 - Reconnaissance Types Detected query 102
 - Reconnaissance Types Detected trend 105
 - Reconnaissance Types Detected Trend query 104
 - Reconnaissance Types Detected Trend report 97
 - Regulated Systems - By Attack query 107
 - Regulated Systems - By Attack report 107
 - Regulated Systems - By Host - Attacked query 108
 - Regulated Systems - By Host - Attacked report 106
 - Regulated Systems - Count Vulnerabilities query 108
 - Regulated Systems - Count Vulnerabilities report 106
 - Regulated Systems resource group 106
 - Regulated Systems use case 154
 - Repetitive Firewall Block List active list 48
 - reports
 - Access Activity 111
 - Access Events by Database Resource 110
 - Access Events by Email Resource 112
 - Access Events by File Resource 111
 - Access Events by Resource 112
 - Alert Counts by Device 19
 - Alert Counts by Port 19
 - Alert Counts by Severity 20
 - Alert Counts by Type 20
 - Alert Counts per Hour 19
 - Asset Vulnerability List 169
 - Attacker Counts by ArcSight Priority 39
 - Attacker Counts by Attacker Port 38
 - Attacker Counts by Device 40
 - Attacker Counts By Target 38
 - Attacker Counts by Target Port 40
 - Attacker Port Counts 39
 - Bottom N Attack Sources 40
 - Bottom N Attackers 39
 - Bottom N Targets 158
 - Brute Force Access Activity 111
 - Brute Force Session Trends 110
 - Business Role - Attempted Attacks 57
 - Business Role - Successful Attacks 56
 - By User Account - Compromised - Access 158
 - By User Account - Compromised - All Activity 159
 - Connection Counts by User 38, 76
 - Connection Durations by User 76
 - Daily Top 10 Resource Access Trends 113
 - Daily Top 10 Vulnerabilities in Events Trend 169
 - Database Resource Access by Users 111
 - Denied Inbound Connections by Address 39
 - Denied Inbound Connections by Port 40
 - Denied Inbound Connections per Hour 38
 - Denied Outbound Connections by Address 39
 - Denied Outbound Connections by Port 37
 - Denied Outbound Connections per Hour 38
 - Device SNMP Authentication Failures 75
 - Email Resource Access by Users 111
 - Environment Status Events over the Last 24 Hours 67
 - Errors Detected in Anti-Virus Deployment 23
 - Failed Anti-Virus Updates 23
 - Failed Login Attempts 75
 - Failed Logins by Destination Address 76
 - Failed Logins by Source Address 77
 - Failed Logins by User 76
 - File Resource Access by Users 112
 - Inbound DoS Events - Yesterday 60
 - Login Errors by User 77
 - Login Event Audit 75
 - Number of Failed Logins - Daily 123
 - Number of Failed Logins - Today 124
 - Number of Failed Logins - Weekly 123
 - Port Scanning Activity 98
 - Port Scanning Activity Trend 96
 - Prioritized Attack Counts by Service - Last 24 Hours 29
 - Prioritized Attack Counts by Target Zone - Last 24 Hours 29
 - Prioritized Scanning Activity by Business Role 97
 - Prioritized Scanning Activity by Zone 97
 - Recent Activity Affecting Target Assets in Compromised List 157
 - Recent Activity Affecting Target Assets in Hit List 159
 - Recent Activity Affecting Target Assets in Scanned List 156
 - Reconnaissance Types Detected by Zone 98
 - Reconnaissance Types Detected Trend 97
 - Regulated Systems - By Attack 107
 - Regulated Systems - By Host - Attacked 106
 - Regulated Systems - Count Vulnerabilities 106
 - Resource Access by Users 112
 - Resource Access Trend 110
 - Revenue Generating Systems - Attacked 119
 - Revenue Generating Systems - Compromise - All 119
 - Revenue Generating Systems - Compromise - Avail-

- ability 120
- Revenue Generating Systems - Compromise - Confidentiality 120
- Revenue Generating Systems - Compromise - Integrity 120
- SANS Top 20 (v6.01) Attacked Systems - Hourly Report 130
- SANS Top 20 (v6.01) Vulnerability Area Activity - Hourly Report 129
- Sarbanes-Oxley - Top 10 Targets 107
- Scanning Activity by Business Role Trend 96
- Scanning Activity by Zone Trend 97
- Security Intelligence Status Report 147
- Successful Logins by Destination Address 76
- Successful Logins by Source Address 77
- Successful Logins by User 75
- Target Counts by ArcSight Priority 157
- Target Counts by Attacker 157
- Target Counts by Attacker Port 37
- Target Counts by Device 159
- Target Counts by Event Name 159
- Target Counts by Target Port 159
- Target Port Counts 157
- Targets in Compromised List 157
- Targets in Hit List 158
- Targets in Scanned List 156
- Top 10 Talkers 123
- Top 10 Vulnerable Systems - Today 122
- Top 10 Vulnerable Systems - Weekly 124
- Top 5 IDS Signature Destinations per Day 123
- Top 5 IDS Signature Sources per Day 123
- Top 5 IDS Signatures per Day 122
- Top 5 Users with Failed Logins - Daily 124
- Top 5 Users with Failed Logins - Today 122
- Top 5 Users with Failed Logins - Weekly 124
- Top Alert Destinations 158
- Top Alert Sources 39
- Top Alerts from IDS and IPS 19, 122
- Top Application Status Events over the Last 24 Hours 68
- Top Attacker Ports 38
- Top Attackers 39
- Top Hosts by Number of Connections 77
- Top Infected Systems 23
- Top N Attack Signatures Targeting Windows Assets 156
- Top N Attack Sources 39
- Top N Attacked Assets in North America 158
- Top N Attacker Details 38
- Top N Targets (3D Pie Chart) 157
- Top N Targets (Bar Chart) 156
- Top N Targets (Inverted Bar Chart) 159
- Top N Targets (Pie Chart) 158
- Top N Targets (Table and Chart) 158
- Top N Targets (Table) 157
- Top N Vulnerabilities on Assets 169
- Top OS Status Events over the Last 24 Hours 68
- Top Service Status Events over the Last 24 Hours 68
- Top Target IPs 124
- Top Target Ports Chart 157
- Top Targets 158
- Top Users by Average Session Length 37
- Top Vulnerabilities in Events Trend 169
- Total Number of Vulnerable Systems - Monthly 123
- Total Number of Vulnerable Systems - Yearly 123
- Trend: Environment Status Events - Yesterday 67
- Trend: Inbound DoS Events - Yesterday 60, 129
- Trend: Prioritized Attack Counts by Service - Last 24 Hours 29
- Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours 30
- Trend: Top Application Status Events over the Last 24 Hours 67
- Trend: Top OS Status Events over the Last 24 Hours 67
- Trend: Top Service Status Events over the Last 24 Hours 68
- Update Summary 23
- User Activity 76
- Virus Activity by Time 23
- Vulnerabilities and Assets 169
- Vulnerabilities in Events by Zone 169
- Vulnerability Scanner Logs - by Host 123
- Vulnerability Scanner Logs - by Vulnerability 124
- Windows Events 76
- Worm Infected Systems 175
- Resource Access Attempts query 116
- Resource Access by Users report 112
- Resource Access field set 114
- Resource Access Initiation rule 113
- Resource Access on Trend query 116
- Resource Access resource group 109
- Resource Access session list 117
- Resource Access Termination rule 113
- Resource Access trend 118
- Resource Access Trend query 117
- Resource Access Trend report 110
- Resource Accesses query 115
- resource groups
 - Alerts from IDS-IPS 19
 - Anti-Virus Activity and Status 22
 - Attack Rates 27
 - Attackers 37
 - Business Impact Analysis 54
 - DoS 59
 - Environment State 66
 - Login Tracking 74
 - Reconnaissance 95
 - Regulated Systems 106
 - Resource Access 109
 - Revenue Generating Systems 119
 - SANS Top 20 129
 - SANS Top 5 Reports 122
 - Security Overview 145
 - Targets 155
 - Vulnerability 168
 - Worm Outbreak 174
- Revenue Generating Systems - Attacked query 121
- Revenue Generating Systems - Attacked report 119
- Revenue Generating Systems - Compromise - All query 121
- Revenue Generating Systems - Compromise - All report 119
- Revenue Generating Systems - Compromise - Availability query 121
- Revenue Generating Systems - Compromise - Availability report 120
- Revenue Generating Systems - Compromise - Confidentiality query 121

- Revenue Generating Systems - Compromise - Confidentiality report 120
 - Revenue Generating Systems - Compromise - Integrity query 121
 - Revenue Generating Systems - Compromise - Integrity report 120
 - Revenue Generating Systems resource group 119
 - Revenue Generating Systems use case 153
 - Revenue Generation asset category 120, 148
 - Role asset category 148
 - rules
 - Application Brute Force Logins 44
 - Attack from Source having Reconnaissance History 99
 - Attack From Suspicious Source 45
 - Blaster DDOS From Infected Host 175
 - Blaster Infected Host 176
 - Brute Force Logins 41
 - Brute Force Resource Access Initiation 114
 - Firewall - Application Protocol Scan 98
 - Firewall - High Volume Accepts 44
 - Firewall - Host Port Scan 98
 - Firewall - Network Port Scan 99
 - Firewall - Pass After Repetitive Blocks 42
 - Firewall - Repetitive Block - In Progress 42
 - High Number of IDS Alerts for Backdoor 42
 - High Number of IDS Alerts for DoS 61
 - Multi Host Application Brute Force Logins 43
 - Multiple Login Attempts to Locked Windows Account 44
 - Multiple Windows Logins by Same User 47
 - Notify on Successful Attack 44
 - Possible DoS on Hosts 60
 - Possible DoS on Network 61
 - Possible DoS on Services 61
 - Possible Internal Network Sweep 176
 - Possible Outbound Network Sweep 176
 - Probable Attack - Script Attack 47
 - Probable Successful Attack - Brute Force 47
 - Probable Successful Attack - DoS 43
 - Probable Successful Attack - Execute 46
 - Probable Successful Attack - Exploit 42
 - Probable Successful Attack - Information Leak 46
 - Probable Successful Attack - Probable Redirect Attack 45
 - Probable Successful Attack - Repetitive Exploit Events 40
 - Probable Successful Attack - System Configuration 41
 - Resource Access Initiation 113
 - Resource Access Termination 113
 - SANS Top 20 Email (v6.01) - Microsoft Office XP Buffer Overflow Vulnerabilities 134
 - SANS Top 20 Email (v6.01) - Microsoft OLE and COM Remote Code Execution Vulnerabilities 142
 - SANS Top 20 OS (v6.01) - Microsoft Exchange SMTP Service Vulnerabilities 139
 - SANS Top 20 OS (v6.01) - Microsoft License Logging Service Vulnerabilities 138
 - SANS Top 20 OS (v6.01) - Microsoft Message Queuing Service Vulnerabilities 141
 - SANS Top 20 OS (v6.01) - Microsoft MSDTC and COM Service Vulnerabilities 140
 - SANS Top 20 OS (v6.01) - Microsoft NetDDE Service Vulnerabilities 136
 - SANS Top 20 OS (v6.01) - Microsoft NNTP Service Vulnerabilities 137
 - SANS Top 20 OS (v6.01) - Microsoft Plug and Play Service Vulnerabilities 135
 - SANS Top 20 OS (v6.01) - Microsoft SMB Service Vulnerabilities 133
 - SANS Top 20 OS (v6.01) - Microsoft Task Scheduler Service Vulnerabilities 131
 - SANS Top 20 OS (v6.01) - Microsoft WINS Vulnerabilities 132
 - Successful Windows Login 78
 - Successful Windows Logout 78
 - Suspicious Activity - Excess Suspicious Activity 45
 - Suspicious Activity - Packet Manipulation 41
 - Suspicious Activity - Suspicious File Activity 47
 - Suspicious Communication From Attacked Target 45
 - SYN Flood Detected by IDS or Firewall 61
 - Traffic From Dark Address Space 40
 - Traffic To Dark Address Space 159
 - User Session (Accounting User) Started 77
 - User Session (Accounting User) Stopped 78
 - User Session (Administrative User) Started 78
 - User Session (Administrative User) Stopped 77
 - User Session (Normal User) Started 79
 - User Session (Normal User) Stopped 78
 - User VPN Session Started 79
 - User VPN Session Stopped 79
 - Windows Account Created 79
 - Windows Account Created and Deleted within 1 Hour 46
 - Windows Account Locked Out 78
 - Windows Account Locked Out Multiple Times 43
 - Worm Outbreak Detected 175
- S**
- SANS Top 20 (v6.01) Attacked Systems - hourly query 143
 - SANS Top 20 (v6.01) Attacked Systems - Hourly Report report 130
 - SANS Top 20 (v6.01) Vulnerability Area Activity - Hourly Report report 129
 - SANS Top 20 Email (v6.01) - Microsoft Office XP Buffer Overflow Vulnerabilities rule 134
 - SANS Top 20 Email (v6.01) - Microsoft OLE and COM Remote Code Execution Vulnerabilities rule 142
 - SANS Top 20 OS (v6.01) - Microsoft Exchange SMTP Service Vulnerabilities rule 139
 - SANS Top 20 OS (v6.01) - Microsoft License Logging Service Vulnerabilities rule 138
 - SANS Top 20 OS (v6.01) - Microsoft Message Queuing Service Vulnerabilities rule 141
 - SANS Top 20 OS (v6.01) - Microsoft MSDTC and COM Service Vulnerabilities rule 140
 - SANS Top 20 OS (v6.01) - Microsoft NetDDE Service Vulnerabilities rule 136
 - SANS Top 20 OS (v6.01) - Microsoft NNTP Service Vulnerabilities rule 137
 - SANS Top 20 OS (v6.01) - Microsoft Plug and Play Service Vulnerabilities rule 135
 - SANS Top 20 OS (v6.01) - Microsoft SMB Service Vulnerabilities rule 133
 - SANS Top 20 OS (v6.01) - Microsoft Task Scheduler Ser-

vice Vulnerabilities rule 131
 SANS Top 20 OS (v6.01) - Microsoft WINS Vulnerabilities rule 132
 SANS Top 20 resource group 129
 SANS Top 5 Reports resource group 122
 Sarbanes-Oxley - Top 10 Targets query 107
 Sarbanes-Oxley - Top 10 Targets report 107
 Sarbanes-Oxley asset category 107
 Scanned List active list 99, 160
 Scanner Events filter 125, 170
 Scanning Activity by Business Role Trend report 96
 Scanning Activity by Zone Trend report 97
 Security Overview resource group 145
 Security Activity Statistics dashboard 146
 Security Devices asset category 147
 Security Intelligence Status Report report 147
 Service asset category 147
 Service Attacks dashboard 156
 Service Event Counts data monitor 68
 Service Overview active channel 66
 Service-Communications Attacks dashboard 156
 Service-Database Attacks dashboard 155
 Service-Email Attacks dashboard 155
 Services - Communications Service filter 164
 Services - Database Service filter 163
 Services - Email Service filter 164
 Services - Web Service filter 162
 Service-Web Attacks dashboard 155
 session lists
 Brute Force Resource Access 117
 Resource Access 117
 User Sessions 94
 User VPN Sessions 53, 94
 shared libraries 7
 SIS-Assets Compromised Table Query query 153
 SIS-Cases Added Table Query query 153
 SIS-Event Count by Agent Severity Chart Query query 152
 SIS-Notifications Sent Table Query query 153
 SIS-Top Attackers Chart Query query 153
 SIS-Top Attacks Table Query query 153
 SIS-Top Events Table Query query 153
 SIS-Top Firing Rules Table Query query 152
 SIS-Top Target Ports Chart Query query 153
 SIS-Top Targets Chart Query query 153
 SNMP Authentication Failures by Device query 93
 Status by Business Role data monitor 149
 Status by Business Role filter 151
 Status by Development and Operations Roles data monitor 149
 Status by Infrastructure Role data monitor 148
 Status by Revenue Generation Role data monitor 150
 Status by Security Device Role data monitor 149
 Status by Service Role data monitor 150
 Status Overview field set 69
 Successful Attacks filter 58, 152
 Successful Firewall Login Events filter 85
 Successful Inbound Attacks dashboard 156
 Successful Inbound Attacks data monitor 150, 162
 Successful Inbound DoS Events - Trend Filter filter 64, 142
 Successful Inbound DoS Events - Trend query 65, 144
 Successful Inbound DoS Events Last Hour query 65
 Successful Inbound DoS Events Query on Trend query 65, 143

Successful Login by User (Chart) query 94
 Successful Login by User query 92
 Successful Login Events filter 83
 Successful Logins by Destination Address (Chart) query 93
 Successful Logins by Destination Address focused report 87, 88
 Successful Logins by Destination Address report 76
 Successful Logins by Source Address (Chart) query 91
 Successful Logins by Source Address focused report 85, 86, 89, 90
 Successful Logins by Source Address report 77
 Successful Logins by Source-Destination Pair query 94
 Successful Logins by User focused report 86, 87, 88, 90
 Successful Logins by User report 75
 Successful Network Login Events filter 83
 Successful Operating System Login Events filter 83
 Successful VPN Login Events filter 84
 Successful Windows Login filter 49, 84
 Successful Windows Login rule 78
 Successful Windows Logout filter 82
 Successful Windows Logout rule 78
 Suspicious Activity - Excess Suspicious Activity rule 45
 Suspicious Activity - Packet Manipulation rule 41
 Suspicious Activity - Suspicious File Activity rule 47
 Suspicious Communication From Attacked Target rule 45
 Suspicious List active list 48, 99, 159
 SYN Flood Detected by IDS or Firewall rule 61

T

Target Address is NULL filter 24
 Target Asset has Asset Name filter 64, 70, 143
 Target Asset has OS Categorization filter 70
 Target Counts by ArcSight Priority query 165
 Target Counts by ArcSight Priority report 157
 Target Counts by Attacker Port query 52
 Target Counts by Attacker Port report 37
 Target Counts by Attacker query 166
 Target Counts by Attacker report 157
 Target Counts by Device query 167
 Target Counts by Device report 159
 Target Counts by Event Name query 167
 Target Counts by Event Name report 159
 Target Counts by Target Port query 166
 Target Counts by Target Port report 159
 Target Host Name is NULL filter 24
 Target Object starts with Host Application filter 70
 Target Port Activity by Attacker data monitor 177
 Target Port Activity By Attacker filter 177
 Target Port Counts query 166
 Target Port Counts report 157
 Target Port is not NULL filter 34, 64, 70, 142
 Target Service Name is not NULL filter 34, 64, 70, 143
 Target User ID is NULL filter 49, 83
 Target User Name is NULL filter 85
 Target Zone is NULL filter 25
 Targeted Business Impact Analysis filter 57
 Targeted Zones by Service and Customer data monitor 31
 Targeted Zones by Service data monitor 33
 Targets in Compromised List query 166
 Targets in Compromised List report 157
 Targets in Hit List query 165
 Targets in Hit List report 158

- Targets in Scanned List query 164
- Targets in Scanned List report 156
- Targets resource group 155
- TargetUser global variable 82
- Top 10 Alerts focused report 20
- Top 10 Anti-Virus Errors data monitor 23
- Top 10 Application Events data monitor 69
- Top 10 Attack Rate Statistics by Service and Zones dashboard 29
- Top 10 Attack Rate Statistics by Service dashboard 27
- Top 10 Attack Rate Statistics by Zones dashboard 28
- Top 10 Attack Signatures targeting Windows Assets query 165
- Top 10 Attack Sources query 51
- Top 10 Attacked Assets in North America query 165
- Top 10 Attacked Services data monitor 32
- Top 10 Attacker Details query 51
- Top 10 Attacker Zones by Customer data monitor 34
- Top 10 Attacker Zones by Service and Customer data monitor 33
- Top 10 Attacker Zones by Service data monitor 31
- Top 10 Attacker Zones data monitor 32
- Top 10 Attackers focused report 50
- Top 10 Attackers query 50
- Top 10 Communications Service Targets data monitor 162
- Top 10 Customer Attack Rate Statistics by Service and Zones dashboard 28
- Top 10 Customer Attack Rate Statistics by Service dashboard 28
- Top 10 Customer Attack Rate Statistics by Zones dashboard 29
- Top 10 Daily Vulnerabilities in Events on Trend query 171
- Top 10 Daily Vulnerability Events on Trend query 172
- Top 10 Daily Vulnerability Events trend 172
- Top 10 Database Service Targets data monitor 162
- Top 10 Email Service Targets data monitor 161
- Top 10 Infected Systems data monitor 23
- Top 10 Infections data monitor 23
- Top 10 Operating System Events data monitor 69
- Top 10 Reconnaissance Types Detected on Trend query 101
- Top 10 Reconnaissance Types Detected trend 105
- Top 10 Service Events data monitor 69
- Top 10 Talkers query 126
- Top 10 Talkers report 123
- Top 10 Targeted Services by Customer data monitor 33
- Top 10 Targeted Zones by Customer data monitor 32
- Top 10 Targeted Zones by Service and Customer data monitor 31
- Top 10 Targeted Zones by Service data monitor 31
- Top 10 Targeted Zones data monitor 33
- Top 10 Targets focused report 164
- Top 10 Targets query 125, 165
- Top 10 Users With Failed Logins data monitor 80, 81, 82
- Top 10 Vulnerable Systems - Today report 122
- Top 10 Vulnerable Systems - Weekly report 124
- Top 10 Web Service Targets data monitor 162
- Top 10 Zones Scanned data monitor 100
- Top 5 IDS Signature Destinations per Day report 123
- Top 5 IDS Signature Sources per Day report 123
- Top 5 IDS Signatures per Day (Snort-Snort) focused report 125
- Top 5 IDS Signatures per Day report 122
- Top 5 Signatures per Day (CISCO-CiscoSecureIDS) focused report 125
- Top 5 Users with Failed Logins - Daily report 124
- Top 5 Users with Failed Logins - Today report 122
- Top 5 Users with Failed Logins - Weekly report 124
- Top Alert Destinations query 165
- Top Alert Destinations report 158
- Top Alert Sources query 50
- Top Alert Sources report 39
- Top Alerts from IDS and IPS report 19, 122
- Top Anti-Virus Errors query 26
- Top Application Status Events on Trend query 71
- Top Application Status Events over the Last 24 Hours (Chart Query) query 73
- Top Application Status Events over the Last 24 Hours query 72
- Top Application Status Events over the Last 24 Hours report 68
- Top Attacker IPs data monitor 148
- Top Attacker Ports query 50
- Top Attacker Ports report 38
- Top Attackers report 39
- Top Attackers Targeting Critical Assets data monitor 161
- Top Categories data monitor 150
- Top Connection Durations query 92
- Top Connectors data monitor 148
- Top Hosts by Number of Connections focused report 86, 89
- Top Hosts by Number of Connections query 93
- Top Hosts by Number of Connections report 77
- Top IDS and IPS Alerts query 20, 126
- Top IDS Signature Destinations per Day query 127
- Top IDS Signature Sources per Day query 126
- Top IDS Signatures by IDS Product query 126
- Top Infected Systems query 26
- Top Infected Systems report 23
- Top N Attack Signatures Targeting Windows Assets report 156
- Top N Attack Sources report 39
- Top N Attacked Assets in North America report 158
- Top N Attacker Details report 38
- Top N Targets (3D Pie Chart) report 157
- Top N Targets (Bar Chart) report 156
- Top N Targets (Inverted Bar Chart) report 159
- Top N Targets (Pie Chart) report 158
- Top N Targets (Table and Chart) report 158
- Top N Targets (Table) report 157
- Top N Vulnerabilities in Events on Trend query 171
- Top N Vulnerabilities on Assets report 169
- Top Operating System Status Events on Trend query 72
- Top OS Status Events over the Last 24 Hours (Chart Query) query 73
- Top OS Status Events over the Last 24 Hours query 71
- Top OS Status Events over the Last 24 Hours report 68
- Top Service Status Events on Trend query 71
- Top Service Status Events over the Last 24 Hours (Chart Query) query 71
- Top Service Status Events over the Last 24 Hours query 72
- Top Service Status Events over the Last 24 Hours report 68
- Top Status Events on Trend query 71
- Top Target IPs data monitor 149
- Top Target IPs report 124
- Top Target Ports Chart query 167
- Top Target Ports Chart report 157

Top Targets report 158
 Top Transport Protocols data monitor 150
 Top Users by Average Session Length report 37
 Top Users by Connection Count data monitor 81
 Top Users by Connection Count query 53, 92
 Top Users by Login Activity data monitor 80
 Top Users with Failed Logins per Day query 125, 127
 Top Users with Failed Logins per Day trend 127
 Top Users with Failed Logins per Week query 126
 Top VPN Connection Durations query 52
 Top Vulnerabilities in Events Trend report 169
 Top Vulnerable Systems per Week query 126
 Top Zones with Anti-Virus Errors query 25
 Total Number of Vulnerable Systems - Monthly report 123
 Total Number of Vulnerable Systems - Yearly report 123
 Traffic From Dark Address Space rule 40
 Traffic To Dark Address Space rule 159
 Transport Protocol is not NULL filter 34, 65, 71, 143
 Trend: Environment Status Events - Yesterday report 67
 Trend: Inbound DoS Events - Yesterday report 60, 129
 Trend: Prioritized Attack Counts by Service - Last 24 Hours report 29
 Trend: Prioritized Attack Counts by Target Zone - Last 24 Hours report 30
 Trend: Top Application Status Events over the Last 24 Hours report 67
 Trend: Top OS Status Events over the Last 24 Hours report 67
 Trend: Top Service Status Events over the Last 24 Hours report 68
 trends
 Asset Counts by Vulnerability 173
 Brute Force Access Session Trends 118
 Daily Top 10 Resource Access Trends 118
 Environment Status Events 73
 Failed Logins per Hour 128
 Inbound DoS Events 65, 144
 Number of Vulnerabilities per Asset 128
 Port Scanning 105
 Port Scanning Daily Top 20 104
 Prioritized Attack Counts by Service 36
 Prioritized Attack Counts by Target Zone 36
 Prioritized Vulnerability Events by Zone 172
 Reconnaissance Activity 105
 Reconnaissance Types Detected 105
 Resource Access 118
 Top 10 Daily Vulnerability Events 172
 Top 10 Reconnaissance Types Detected 105
 Top Users with Failed Logins per Day 127
 Zone Scanning Events by Priority 105
 Trusted List active list 48, 61, 99, 114, 142, 176

U

Untrusted List active list 48, 99, 176
 Update Events filter 25
 Update Summary Chart query 26
 Update Summary query 26
 Update Summary report 23
 upgrade
 invalid resources 181
 preparing for upgrade 179
 restoring content 180
 verify customer content 181

use cases

 Business Impact Analysis 154
 Environment State 153
 Regulated Systems 154
 Revenue Generating Systems 153
 User Activity query 91
 User Activity report 76
 User Session (Accounting User) Started rule 77
 User Session (Accounting User) Stopped rule 78
 User Session (Administrative User) Started rule 78
 User Session (Administrative User) Stopped rule 77
 User Session (Normal User) Started rule 79
 User Session (Normal User) Stopped rule 78
 User Sessions session list 94
 User VPN Session Started rule 79
 User VPN Session Stopped rule 79
 User VPN Sessions session list 53, 94
 User-based Rule Exclusions active list 48, 79
 Users by Connection Count query 52, 92
 Users with Open Connections query 91
 Users with Open VPN Connections query 53

V

Very High asset category 161
 Very High Criticality Assets filter 163
 Virus Activity by Host data monitor 24
 Virus Activity by Hour query 25
 Virus Activity by Time report 23
 Virus Activity by Zone data monitor 24
 Virus Activity data monitor 23
 Virus Activity filter 24
 Virus Activity Overview dashboard 22
 Virus Activity Statistics dashboard 22
 VPN Events filter 82
 VPN Login Events filter 83
 VPN Login Overview dashboard 74
 Vulnerabilities (by Asset Counts) on Trend query 171
 Vulnerabilities and Assets query 170
 Vulnerabilities and Assets report 169
 Vulnerabilities asset category 142
 Vulnerabilities in Events by Zone (Chart Query) query 170
 Vulnerabilities in Events by Zone report 169
 Vulnerability Events active channel 168
 Vulnerability field set 170
 Vulnerability resource group 168
 Vulnerability Scanner Events active channel 168
 Vulnerability Scanner field set 170
 Vulnerability Scanner Logs - by Host report 123
 Vulnerability Scanner Logs - by Vulnerability report 124
 Vulnerability Scanner Logs query 127

W

Web asset category 160
 Web Service Attack Activity data monitor 161
 Windows Account Created and Deleted within 1 Hour rule 46
 Windows Account Created rule 79
 Windows Account Locked Out Multiple Times rule 43
 Windows Account Locked Out rule 78
 Windows Created Accounts active list 49, 80
 Windows Events query 92
 Windows Events report 76

Windows Locked Out Accounts active list 48, 79
Windows Login Count active list 48, 80
Worm Activity filter 178
Worm Activity Status data monitor 177
Worm Geo Filter filter 178
Worm Infected Machines data monitor 149
Worm Infected Systems active list 114, 176
Worm Infected Systems dashboard 147
Worm Infected Systems data monitor 149, 177
Worm Infected Systems filter 178
Worm Infected Systems query 178
Worm Infected Systems report 175
Worm Outbreak dashboard 174
Worm Outbreak Detected rule 175
Worm Outbreak filter 150, 177
Worm Outbreak Overview dashboard 174

Worm Outbreak resource group 174
Worm Propagation by Host data monitor 177
Worm Propagation by Zone data monitor 177
Worm Spread data monitor 177
Worm Spread Geo View dashboard 174
Worm Traffic filter 152, 178

Z

Zone Scanning Activity on Trend (Chart Query) query 104
Zone Scanning Activity on Trend query 104
Zone Scanning Events by Priority trend 105
Zone Scanning Events by Priority Trend query 103
Zone Scanning Events query 101

