
Micro Focus Security ArcSight ESM

Software Version: 7.2 Service Pack 1

ArcSight Administration and ArcSight System Standard Content Resources

Document Release Date: April 2020

Software Release Date: April 2020



Legal Notices

Copyright Notice

© Copyright 2001-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

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

Contents

Overview	7
ArcSight Administration Resources	8
ArcSight Administration Resources By Type	8
Active Channels	9
Active Lists	10
Dashboards	14
Data Monitors	18
Fields	25
Field Sets	25
Filters	26
Global Variables	33
Integration Commands	37
Integration Configurations	38
Integration Targets	38
Queries	39
Query Viewers	53
Reports	59
Report Templates	69
Rules	70
Session Lists	77
Trends	77
Use Cases	79
ArcSight CORRE Resources By Type	80
Active Lists	80
Dashboards	81
Data Monitors	81
Filters	82
Focused Reports	83
Queries	84
Query Viewers	85
Reports	85
Report Templates	86
Rules	86

Session Lists	87
Use Cases	87
ArcSight Content Management Resources By Type	88
Active Lists	88
Dashboards	88
Queries	89
Query Viewers	90
Reports	91
Rules	92
Notification Groups	92
Use Cases	92
Transformation Hub Monitoring Resources by Type	93
Active Channels	93
Active Lists	93
Dashboards	94
Data Monitors	94
Field Sets	94
Filters	95
Queries	95
Query Viewers	95
Rules	96
ESM Active Passive High Availability (APHA) Monitoring Resources By Type	97
Active Channels	97
Active Lists	97
Dashboards	98
Data Monitors	98
Field Sets	98
Filters	100
Queries	100
Query Viewers	101
Reports	101
Rules	102
Session Lists	102
Use Cases	102
ArcSight Foundation Resources	103
ArcSight ClusterView Resources By Type	105
Data Monitors	105

Fields	106
ArcSight SOCVIEW Resources By Type	107
Data Monitors	107
Filters	108
Query Viewers	108
Queries	108
Security Threat Monitoring Resources By Type	109
Fields	110
Field Sets	111
Active Channels	112
Active Lists	113
Dashboards	114
Data Monitors	115
Filters	117
Packages	120
Queries	121
Query Viewers	122
Rules	123
Use Cases	127
Security Monitoring - Base Resources By Type	129
Active Channels	130
Active Lists	131
Data Monitors	132
Dashboards	133
Fields	134
Field Sets	136
Filters	137
Integration Commands	138
Integration Configurations	139
Packages	140
Queries	141
Query Viewers	142
Rules	143
Reports	144
Use Cases	145
Security Monitoring - Base - Active Lists Resources By Type	146
Active Lists	147
Packages	148

Threat Intelligence Platform Resources By Type	149
Filters	150
Fields	151
Active Lists	158
Integration Commands	160
Integration Configurations	161
Packages	162
Rules	163
Dashboards	166
Queries	167
Query Viewers	168
Use Cases	169
Common Resources By Type	170
Conditional Variable Filters	170
Network Filters	179
Variables Library Fields	180
ArcSight System Resources	187
Active Channels	187
Active Lists	188
Destinations	189
Field Sets	190
Filters	192
Integration Commands	196
Integration Configurations	197
Queries	199
Reports	200
Rules	201
Send Documentation Feedback	203

Overview

This document lists a series of standard content resources, such as dashboards, active channels, reports, filters, rules, etc. The resources are designed to give you pre-installed comprehensive correlation, monitoring, reporting, alerting, and case management with minimal configuration.

The standard content resources are installed using a series of packages (.arb files), some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options.

For detailed information about using ArcSight ESM, see the ArcSight ESM documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Security Use Case Guides, Release Notes, and individual SmartConnector Guides are available on the [ArcSight Documentation page](#).

ArcSight Administration Resources

This chapter lists all the resources by type in the ArcSight Administration packages.

• ArcSight Administration Resources By Type	8
• ArcSight CORRE Resources By Type	80
• ArcSight Content Management Resources By Type	88
• Transformation Hub Monitoring Resources by Type	93
• ESM Active Passive High Availability (APHA) Monitoring Resources By Type	97

ArcSight Administration Resources By Type

This section lists all the resources by type.

• Active Channels	9
• Active Lists	10
• Dashboards	14
• Data Monitors	18
• Fields	25
• Field Sets	25
• Filters	26
• Global Variables	33
• Integration Commands	37
• Integration Configurations	38
• Integration Targets	38
• Queries	39
• Query Viewers	53
• Reports	59
• Report Templates	69
• Rules	70
• Session Lists	77
• Trends	77
• Use Cases	79

Active Channels

The following table lists all the active channels.

Active Channel Resources

Resource	Description	URI
ASM Events	This active channel shows ArcSight System Monitoring events generated by the local ArcSight ESM system.	/All Active Channels/ArcSight Administration/ESM/System Health/Events/
Actor Audit Events	This active channel displays events in which there are changes to data in the actor resources.	/All Active Channels/ArcSight Administration/ESM/Configuration Changes/Actors/
ArcSight ESM Device Monitoring	This active channel shows device status events.	/All Active Channels/ArcSight Administration/Devices/
Connector Caching Events	This active channel displays information about Connector cache status audit events and correlation events from the related Connector Monitoring rules.	/All Active Channels/ArcSight Administration/Connectors/System Health/
Connector Connection Status Events	This active channel displays information about connector connection status audit events and correlation events from the related Connector Monitoring rules.	/All Active Channels/ArcSight Administration/Connectors/System Health/
Connector Upgrades	This active channel shows all the events related to connector upgrades within the last two hours. The active channel uses the Connector Upgrades field set.	/All Active Channels/ArcSight Administration/Connectors/Configuration Changes/
Distributed Correlation Events	This active channel shows distributed correlation audit events.	/All Active Channels/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Logger Application Events	This active channel shows all the Logger application events within the last hour.	/All Active Channels/ArcSight Administration/Logger/
Logger Platform Events	This active channel shows all the Logger platform events within the last hour.	/ArcSight Administration/Logger/

Active Channel Resources, continued

Resource	Description	URI
Logger System Health Events	This active channel shows all the Logger system health events within the last hour.	/All Active Channels/ArcSight Administration/Logger/
Query Viewers Status	This active channel shows all the query viewer-related events within the last two hours.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/
Reports Status	This active channel shows all the report-related events within the last two hours.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/
System Events Last Hour	This active channel shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlated events.	/All Active Channels/ArcSight Administration/ and /All Active Channels/ArcSight Administration/ESM/System Health/Events/
Trends Status	This active channel shows all the trend-related events within the last two hours. The Trend Name field shows the name of the Trend and the URI. The Trend Infos field shows information on the Trend event.	/All Active Channels/ArcSight Administration/ESM/System Health/Resources/

Active Lists

The following table lists all the active lists.

Active List Resources

Resource	Description	URI
All Monitored Devices	This active list is populated by the All Monitored Devices rule. The active list stores entries for 365 days and is used by queries to retrieve device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Average EPS	This active list stores average EPS during last hour.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Black List - Connectors	This active list maintains a list of connectors that are not monitored by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/

Active List Resources, continued

Resource	Description	URI
Black List - Reverse Look Up	This active list stores look-up data to enable the rules to update the connector connection and caching status displays when a connector is added to the Black List - Connectors active list. Note: This list should contain all the information that is also included in the Connector Information active list. This active list links the information in the Black List - Connectors active list to the information in the Connector Information active list. The connectors listed in the Black List - Connectors active list are the only ones not processed by the Connector Monitoring rules. Do not edit the entries in this list unless you are sure that an entry is no longer valid (and can be removed).	/All Active Lists/ArcSight Administration/Connectors/System Health/Custom/
Connector Average EPS - Last 7 Days	This active list stores the average EPS for all connectors during the last seven days. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/
Connector Daily Average EPS	This active list stores the daily average EPS for all connectors. The data is from a trend.	/All Active Lists/ArcSight Administration/Connectors/System Health/EPS/
Connector Information	This active list maintains a list of the available information about connectors, whether they are directly connected to an ESM manager or indirectly through a Logger. Note: Information is derived from connector audit events and some information might be incomplete (blank) until the appropriate audit event arrives and is processed by the Connector Monitoring rules.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connector Upgrades	This active list stores information related to successful and failed connector upgrades. When an upgrade is successful, the active list stores the Upgrade Time, Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. When an upgrade fails, the active list also stores the reason for the failure. The active list is populated by the Connector Upgrade Failed and Connector Upgrade Successful rules.	/All Active Lists/ArcSight Administration/Connectors/Configuration Changes/

Active List Resources, continued

Resource	Description	URI
Connectors - Caching	This active list stores information about the connectors that are currently caching events. A connector is removed from the active list when the cache is empty again or when it has been caching for more than two hours (by default).	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Down	This active list stores the IDs and names of connectors that are currently down (either a connector shut down or a heartbeat timeout). After the TTL of the active list expires, the connector information is added to the Connectors Still Down active list and a notification is sent to the SOC Operators to inform them that the connector has been down for 20 or more minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Dropping Events	This active list stores the connectors that are currently dropping events (for example, when the cache is full). The connector is removed from the active list when the cache is empty again.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Still Caching	This active list stores available information about connectors that have been caching for over two hours (by default).	/All Active Lists/ArcSight Administration/Connectors/System Health/
Connectors - Still Down	This active list stores the ID and the name of the connectors that are have been down for 20 minutes or more (either a connector shut down or a heartbeat timeout). After the TTL of the Connectors - Down active list expires, the connector information is added to this list and a notification is sent to the SOC Operators to inform them that the connector has been down for more than 20 minutes. The connector is removed from the active list when it restarts or reconnects.	/All Active Lists/ArcSight Administration/Connectors/System Health/
Counts from Distributed Correlation	No description available.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Counts in Persistor	No description available.	/All Active Lists/ArcSight Administration/ESM/Distributed Correlation Monitoring/

Active List Resources, continued

Resource	Description	URI
Critical Devices	This active list is populated manually and used by the Critical Monitored Devices rule first. If the rule finds a match, it updates the Critical Monitored Devices active list, which in turn is used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Critical Monitored Devices	This active list is populated manually at first and then updated by the Critical Monitored Devices rule. The entries in this active list never expire, and are used by queries to retrieve critical device activity information by dashboards and reports.	/All Active Lists/ArcSight Administration/Devices/
Invalid Resources	This active list stores a list of resources that become invalid. The Resource Became Invalid rule adds an entry to the active list and the Resource Became Valid rule removes the corresponding entry from the active list.	/All Active Lists/ArcSight Administration/ESM/System Health/Resources/
Logger Sensor Type Status	This active list stores the status of the various hardware sensors on the Loggers. The active list stores the Logger address, the sensor type, the sensor name, and the sensor status. The Logger address and the sensor type are the key fields. This active list is used by a set of rules to identify the status of a sensor type for a Logger.	/All Active Lists/ArcSight Administration/Logger/System Health/
Logger Status	This active list stores the status of the various hardware sensors on the Loggers. The active list stores the Logger address, the sensor type, the sensor name, and the sensor status. The Logger address is the key field. This active list is used by a set of rules to identify the overall status of a Logger.	/All Active Lists/ArcSight Administration/Logger/System Health/
Query Running Time	This active list stores query information used to monitor and report the query duration.	/All Active Lists/ArcSight Administration/ESM/System Health/Resources/
Storage Licensing Data by Connector	This active list stores the raw event length reported by the raw event statistics events for each connector.	/All Active Lists/ArcSight Administration/ESM/Licensing/
Whitelisted Monitored Devices	This active list includes non-critical devices that you want to exclude from monitoring. This list is populated manually. The entries never expire.	/All Active Lists/ArcSight Administration/Devices/

Dashboards

The following table lists all the dashboards.

Dashboard Resources

Resource	Description	URI
Actor Administration	This dashboard shows the Actor Authenticators query viewer.	/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Change Log	This dashboard shows an overview of actor resource changes.	/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Actors/
All Monitored Devices	This dashboard shows an overview of all ESM devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	/All Dashboards/ArcSight Administration/Devices/
ArcSight Appliances Overview	This dashboard shows an overview of all the ArcSight appliances. The dashboard includes the Logger Hardware Status, Logger Disk Usage, Connector Appliance Status, and Connector Appliance Disk Usage data monitors.	/All Dashboards/ArcSight Administration/Logger/
ArcSight User Activity	This dashboard shows login session information and notification activity for ArcSight ESM users.	/All Dashboards/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Status	This dashboard displays the ArcSight User Sessions data monitor, showing recent login/logout activity for users, the remote terminal and zone, and current status.	/All Dashboards/ArcSight Administration/ESM/User Access/User Sessions/
CPU and Memory	This dashboard shows the CPU and memory usage for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Connector Connection and Cache Status	This dashboard displays the overall status of connectors and information on connectors that are down, caching, or dropping events.	/All Dashboards/ArcSight Administration/Connectors/System Health/

Dashboard Resources, continued

Resource	Description	URI
Critical Monitored Devices	This dashboard shows an overview of the critical devices. The green panel shows monitored devices that have been active for the last 20 minutes. The yellow panel shows monitored devices that have been inactive for more than 20 minutes but less than 60 minutes. The red panel shows monitored devices that have been inactive for more than 60 minutes.	/All Dashboards/ArcSight Administration/Devices/
Current Event Sources	This dashboard displays information about the status of your connectors, as well as the top devices (vendor and product) that are contributing events.	/All Dashboards/ArcSight Administration/Connectors/System Health/
Data Monitor Status	<p>This dashboard displays information about the load and performance of data monitors. The dashboard provides information about the top data monitors based on event count, event processing time, distributed cache synchronization count, and distributed cache synchronization time. This dashboard uses data monitors to monitor other data monitors.</p> <p>Data monitors that cause unusual load on the system and reduce event throughput are likely to be displayed on this dashboard.</p> <p>The appearance of a data monitor on this dashboard does not necessarily mean that the data monitor is having a problem. For example, some data monitors from ESM standard content will appear on this dashboard because they are designed to process every event in the system. But, if a user-defined data monitor appears on this dashboard, it should be examined to verify whether its properties are correct. An unusually broad filter, low availability interval, or unnecessary aggregate fields are possible reasons for a data monitor to cause unusual load.</p>	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Data Monitors/
ESM System Information	This dashboard displays the System Information data monitor, which provides version, licensing, system resources availability and statistics, and other important settings and status.	/All Dashboards/ArcSight Administration/ESM/System Health/
Event Count History	This dashboard displays the total number of non-ArcSight events within the last seven days and the last 30 days.	/All Dashboards/ArcSight Administration/ESM/Event Analysis Overview/
Event Overview	This dashboard displays an overview of non-ArcSight events focusing on Events Counts, Events by Connector, Events by Vendor and Product, and Events by Device Address.	/All Dashboards/ArcSight Administration/ESM/Event Analysis Overview/

Dashboard Resources, continued

Resource	Description	URI
Event Throughput	This dashboard displays the Event Throughput and Event Throughput Statistics data monitors, providing an overview of the system activity related to connectors.	/All Dashboards/ArcSight Administration/ESM/System Health/Events/
Hardware	This dashboard shows the status for all the hardware sensors on the Logger defined in the My Logger filter. The dashboard includes the CPU Sensors, FAN Sensors, and System Sensors data monitors.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Latest Events By Priority	This dashboard shows event count distribution ordered by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.	/All Dashboards/ArcSight Administration/ESM/System Health/Events/
My Logger Overview	This dashboard shows an overview of the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the My Logger filter.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Network	This dashboard shows the network and EPS usage for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Query Running Time Overview	This dashboard shows the top ten longest queries for report, trend, and query viewers. The dashboard also shows query counts by type of queries.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Query Viewer Details	This dashboard shows query details for query viewers.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Details	This dashboard shows query details for reports.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Reporting Subsystem Statistics	This dashboard displays the ArcSight Reporting Statistics, Currently Running Reports, and Report Statistics data monitors, providing an overview of the resources and processing time devoted to reports.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/
Resource Change Log	This dashboard shows the changes (add, update, delete) to content resources and detailed information about logs associated with those actions.	/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Resources/

Dashboard Resources, continued

Resource	Description	URI
Rules Status	This dashboard shows status about the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, Sortable Rule Stats, and error logs are shown.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Rules/
Storage	This dashboard shows the disk usage and the disk read/write speed for the Logger defined in the My Logger filter within the last ten minutes and the last hour.	/All Dashboards/ArcSight Administration/Logger/My Logger/
Trend Details	This dashboard shows query details for trends.	/All Dashboards/ArcSight Administration/ESM/System Health/Resources/Reporting/

Data Monitors

The following table lists all the data monitors.

Data Monitor Resources

Resource	Description	URI
Actor Change Log	This data monitor displays the most recent events related to changes in actors. These changes include creation, deletion, and modification of single-valued and multi-valued parameters of actor resources. Note: This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/
Actor Change Overview	This data monitor shows an overview of the actor resource changes. The data monitor shows the total number of changes by type within the last hour.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log/
ArcSight Reporting Statistics	This data monitor shows report statistics for the last 15 minutes. Report statistics include the number of running reports, the number of reports querying the database, and the number of reports rendering. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
ArcSight User Sessions	This data monitor shows the status of the ArcSight user sessions to the ArcSight Manager. The data monitor shows the username, the IP address of the machine from which the user is connecting, and the status of the connection. The status of the connection can be: Logged in, Logged out, or Login Timed Out.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/ArcSight User Status/
CPU Sensors	This data monitor shows the status for all the CPU sensors on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
CPU Usage (Percent) - Last 10 Minutes	This data monitor shows the CPU usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/

Data Monitor Resources, continued

Resource	Description	URI
CPU Usage (Percent) - Last Hour	This data monitor shows the CPU usage for the Logger defined in the My Logger filter for the last hour. This Data Monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Connector Cache Status	This data monitor shows the current status of caching across all connectors. If one or more connectors has been caching for longer than two hours (by default), the status is yellow (long-term caching). If one or more connectors is dropping events, the status is red.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
Connector Connection Status	This data monitor shows the current status of the connector connections across all connectors. If one or more connectors is down for less than 20 minutes (by default), the status is yellow (short-term outage). If one or more connectors is down for longer than 20 minutes, the status is red (long-term outage).	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Connection and Cache Status/
Current Connector Status	This data monitor displays information about the connectors that are registered with the system and reporting events.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/
Current Users Logged In	This data monitor shows information about the users currently logged into the ArcSight ESM system.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
Currently Running Reports	This data monitor shows report statistics for currently running reports.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Database Transaction Volume	This data monitor shows transaction settings and detailed information about database transactions.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/
Disk Read and Write (Kbytes per Second) - Last 10 Minutes	This data monitor shows the disk read/write speed for the Logger defined in the My Logger filter for the last 10 minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/

Data Monitor Resources, continued

Resource	Description	URI
Disk Read and Write (Kbytes per Second) - Last Hour	This data monitor shows the disk read/write speed for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage/
Disk Usage	This data monitor shows the disk status for the Logger defined in the My Logger filter. The state can be normal, warning, or critical, based on the disk free space. This Data Monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Disk Usage (Percent)	This data monitor shows the disk free space for the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage/
EPS Usage (Events per Second) - Last 10 Minutes	This data monitor shows the EPS usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
EPS Usage (Events per Second) - Last Hour	This data monitor shows the EPS usage for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Network/
Event Counts	This data monitor shows all non-ArcSight events	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Event Throughput	This data monitor shows the average EPS (events per second) for all the events within the last hour. The sampling interval is five minutes.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Event Throughput/
Event Throughput Statistics	This data monitor shows event throughput from various connectors sending events to this ArcSight ESM.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Event Throughput/
Events By Priority	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/

Data Monitor Resources, continued

Resource	Description	URI
Events by Connector	This data monitor shows the total number of non-ArcSight events by connector.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Events by Device Address	This data monitor shows all non-ArcSight events by device address.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
Events by Vendor and Product	This data monitor shows all non-ArcSight events by vendor and product.	/All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
FAN Sensors	This data monitor shows the status for all the FAN sensors on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
Last 10 Trend Queries Returning No Results	This data monitor shows the last ten trend queries that return no results.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Trends/
Latest Elevated Threat Events	This data monitor shows the list of critical devices that are currently down. A device is down if it has not reported for a certain period of time (30 minutes by default).	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Guarded Threat Events	This data monitor shows detailed information about the latest threat events with a priority level of 3 or 4.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest High Threat Events	This data monitor shows detailed information about the latest threat events with a priority level of 7 or 8.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Low Threat Events	This data monitor shows detailed information about the latest threat events with a priority level less than or equal to 2.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Latest Severe Threat Events	This data monitor shows detailed information about the latest threat events with a priority level greater than 8.	/All Data Monitors/ArcSight Administration/ESM/System Health/Events/Latest Events By Priority/
Logger Disk Usage	This data monitor shows the disk status for all Loggers. The state can be normal, warning, or critical, based on the disk free space. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview/

Data Monitor Resources, continued

Resource	Description	URI
Logger Hardware Status	This data monitor shows the overall hardware status for all Loggers. The state is green (OK) if all the hardware sensors for a Logger are OK, red (NOT OK) if any of the sensors are not OK. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview/
Memory Usage (Mbytes per Second) - Last 10 Minutes	This data monitor shows the memory usage (JVM, Platform) for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Memory Usage (Mbytes per Second) - Last Hour	This data monitor shows the memory usage (JVM, Platform) for the Logger defined in the My Logger filter for the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory/
Network Usage (Bytes) - Last 10 Minutes	This data monitor shows the network usage for the Logger defined in the My Logger filter within the last ten minutes. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Network Usage (Bytes) - Last Hour	This data monitor shows the network usage for the Logger defined in the My Logger filter within the last hour. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Network/
Notification Log	This data monitor shows notification activity generated by ArcSight ESM rules. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/
Partial Matches per Rule	This data monitor shows event counts for partial rule matches.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Recent Fired Rules	This data monitor shows detailed information about the most recently fired rules.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Data Monitor Resources, continued

Resource	Description	URI
Recent System Resource Deletes	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/
Recent System Resource Inserts	This data monitor does not populate all values when running in Turbo Mode Fastest.	/ArcSight Administration/ESM/Configuration Changes/Resources/
Recent System Resource Updates	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/
Report Statistics	This data monitor shows reporting statistics related to runtimes for currently running and past run reports.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Reporting/Reporting Subsystem Statistics/
Resource Change Log	This data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Resource Change Overview	This data monitor shows an overview of the ArcSight resource changes (the total number of changes by type within the last hour).	/All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Resources/Resource Change Log/
Rule Error Logs	This data monitor shows the most recent errors received from the rules engine.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Sensor Type Status	This data monitor shows the hardware status by sensor type for the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview/
Sortable Rule Stats	<p>This data monitor shows statistics for rule performance, such as partial matches, matching events, correlation events, time to execute, and memory used by each rule. You can sort the information in each column by clicking the column title.</p> <p>Note: Lightweight rules do not use in-memory operations or data field aggregation, and do not generate correlation events. Therefore, Matching Events, Correlation Events, and Aggregation Sets are always zero for lightweight rules.</p>	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/

Data Monitor Resources, continued

Resource	Description	URI
System Information	This data monitor shows detailed system information about this ArcSight ESM.	/All Data Monitors/ArcSight Administration/ESM/System Health/ESM System Information/
System Sensors	This data monitor shows the status for all the hardware sensors that are not CPUs or FANs on the Logger defined in the My Logger filter. This data monitor is disabled by default. Enable the data monitor if you have Logger in your environment.	/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware/
Top Event Sources	This data monitor shows the most common event generating products and displays a listing of the top 20.	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/
Top Firing Rules	This data monitor shows detailed information about the top firing rules.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Rules/Rules Status/
Top Data Monitors by Event Count	This data monitor shows the top data monitors by event count.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Data Monitors/Data Monitor Status/
Top Data Monitors by Event Processing Time	This data monitor shows the top data monitors by event processing time.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Data Monitors/Data Monitor Status/
Top Data Monitors by DCache Sync Count	This data monitor shows the top data monitors by distributed cache synchronization count.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Data Monitors/Data Monitor Status/
Top Data Monitors by DCache Sync Time	This data monitor shows the top data monitors by distributed cache synchronization time.	/All Data Monitors/ArcSight Administration/ESM/System Health/Resources/Data Monitors/Data Monitor Status/
User Access Log	This data monitor shows recent user session data events. The data monitor does not populate all values when running in Turbo Mode Fastest.	/All Data Monitors/ArcSight Administration/ESM/User Access/User Sessions/Console and ArcSight Web Status/

Fields

The following table lists all the fields.

Field Resources

Resource	Description	URI
Service Message	This variable returns service message for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/
serviceNameAndId	This variable returns name and ID for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/

Field Sets

The following table lists all the field sets.

Field Set Resources

Resource	Description	URI
ASM Events	This field set contains fields of interest for monitoring ASM events.	/All Field Sets/ArcSight Administration/ESM/
Actor Audit Field Set	This field set contains fields of interest for monitoring changes to actor resources.	/All Field Sets/ArcSight Administration/ESM/Actor/
ArcSight ESM Device Monitoring	This field set contains fields used to examine device status events.	/All Field Sets/ArcSight Administration/Devices/
Connector Monitoring Events	This field set contains fields used to examine connector monitoring events, such as specific connector audit events and correlation events resulting from rules in the Connector Monitoring use cases.	/All Field Sets/ArcSight Administration/Connector/
Connector Upgrades	This field set is used by the Connector Upgrades active channel. The selected fields are: Manager Receipt Time, End Time, Name, Device Event Category, Agent Name, Agent Version, Agent Address, and Agent Zone Name.	/All Field Sets/ArcSight Administration/Connector/
Distributed Correlation Events	This field set is for distributed correlation monitoring.	/All Field Sets/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Logger Application Events	This field set is used by the Logger Application Events active channel. The field set identifies the end time, event name, Logger user, client address (browser), and Logger address.	/All Field Sets/ArcSight Administration/Logger/

Field Set Resources, continued

Resource	Description	URI
Logger Platform Events	This field set is used by the Logger Platform Events active channel. The field set selects the end time, event name, Logger user, client address (browser), and Logger address.	/All Field Sets/ArcSight Administration/Logger/
Logger System Health Events	This field set is used by the Logger System Health Events active channel. The field set identifies the end time, the Logger address, the device event category, the value, unit, time frame, and status of the system health events.	/ArcSight Administration/Logger/
Query Status	This field set displays detailed information about queries.	/All Field Sets/ArcSight Administration/ESM/

Filters

The following table lists all the filters.

Filter Resources

Resource	Description	URI
Aggregator Audit Events	This filter selects audit events for aggregator.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
ASM Asset Resolution Timings	This filter detects ArcSight Status Monitor events that contain asset resolution timing information. The asset resolution average time is the average time in milliseconds taken to resolve an end-point in an event to an asset.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Assets/
ASM CPU Load	This filter identifies ArcSight ESM monitoring events related to CPU load.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Database Load Statistics	This filter identifies events related to ArcSight ESM database load.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Database Statistics	This filter identifies events related to ArcSight ESM database statistics (such as insertion/retrieval).	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Event Evaluation	This filter identifies ArcSight ESM events based on rule insert event rates, data monitor evaluations per second, and filter evaluation counts.	/All Filters/All Filters/ArcSight Administration/ESM/System Health/Resources/

Filter Resources, continued

Resource	Description	URI
ASM Event Flow	This filter captures events that identify the ESM load through flow levels of events.	/All Filters/ArcSight Administration/ESM/System Health/Events/
ASM Flow Load	This filter identifies ArcSight ESM monitoring events related to event flow.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Load Overview	This filter captures events that identify the load associated with the ArcSight ESM system through various parameters such as CPU, database, flow levels, memory, and resources.	/All Filters/ArcSight Administration/ESM/System Health/
ASM Reports Statistics	This filter detects Status Monitor events containing report statistics information. These events provide statistics about the current number of reports querying the database or being rendered.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Reporting/
ASM Resource and Memory Load	This filter identifies ArcSight ESM monitoring events related to resource and memory load.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Sidetable Cache Hit Rates	This filter detects ArcSight System Monitor events that contain side table cache hit rate information. Side tables are tables held in memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The cache hit rate identifies how many successful attempts were made to find entries within the past two hours.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Sidetable Sizes	This filter identifies ArcSight System Monitor events that contain side table size information. Side tables are tables held in-memory and in the database to retain common and relatively static information, such as geographical information, categorization information, connector information, device information, and labels for custom strings and numbers. The side table size identifies how many entries are currently in the cache.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
ASM Standing Load	This filter identifies currently active, data monitor, rules, and active channel related events.	/All Filters/ArcSight Administration/ESM/System Health/Resources/
ASM Total Asset Count	This filter detects ArcSight System Monitor events that contain the current total number of assets.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Assets/

Filter Resources, continued

Resource	Description	URI
Actor Changes	This filter detects actor resource audit events.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
Actor Deletes	This filter detects deleted actor resources. Note: This filter only detects deleted actor events and ignores deleted entries for multi-value parameters.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
Actor Inserts	This filter detects new actor resources. Note: This filter searches for new actors only and ignores new entries for multi-value parameters.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
Actor Name or UUID	This filter detects actor audit events in which the file name is a UUID. If the file name is a UUID, an actor is returned and the full name is available. Otherwise, the field is either not a UUID or the actor resource is not in the system.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
Actor Updates	This filter detects changes to the actor resources. Note: Actors can have three types of updates: an update to a single value parameter, and an addition or deletion of multi-value parameters.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Actor Update Tracking/
ArcSight Audit Events	This filter captures ArcSight ESM audit events.	/All Filters/ArcSight Administration/ESM/System Health/Events/Audit/
ArcSight Login Events	This filter selects events that are associated with logins to the ArcSight ESM system.	/All Filters/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight Login Rule Firings	This filter identifies events that contain ArcSight login rule triggering information. The deviceEventCategory used in this filter is generated by the ArcSight User Login rule. The filter is used by a trend that tracks hourly login statistics.	/All Filters/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight Login Tracking	This filter identifies events that contain ArcSight login and logout information. The device event class IDs used in this filter are generated by the ArcSight auditing system.	/All Filters/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight Rules	This filter identifies ArcSight ESM correlation events generated by rules.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Rules/
ArcSight Status Monitoring Events	This filter selects ArcSight Status Monitoring events generated by the local ArcSight ESM system.	/All Filters/ArcSight Administration/ESM/System Health/

Filter Resources, continued

Resource	Description	URI
Correlator Audit Events	This filter selects audit events for correlator.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
CPU Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is CPU for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/
CPU Usage	This filter identifies Logger system health events related to CPU usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/CPU and Memory/
Connector Cache Status	This filter detects correlation events from the Update Connector Caching Status rule.	/All Filters/ArcSight Administration/Connectors/System Health/
Connector Caching Event	This filter detects connector caching events.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
Connector Connection Status	This filter detects correlation events related to connector connection status.	/All Filters/ArcSight Administration/Connectors/System Health/
Connector Registered or Heartbeat Event	This filter detects events for connector timeouts because the connector information is not complete in Device Custom String2.	/All Filters/ArcSight Administration/Connectors/System Health/Conditional Variable Filters/
Database Insert Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/InsertTime.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
Database Retrieval Time Statistics	This filter identifies ArcSight system events where the Device Event Category is /Monitor/EventBroker/RetrievalTime.	/All Filters/ArcSight Administration/ESM/System Health/Storage/
Disk Read and Write	This filter identifies Logger system health events related to disk read/write speed that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Storage/
Disk Usage	This filter identifies Logger system health events related to disk usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Storage/

Filter Resources, continued

Resource	Description	URI
Distributed Cache Audit Events	This filter selects audit events for distributed cache.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Distributed Correlation Audit Events	This filter selects audit events for distributed correlation.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
EPS Usage	This filter identifies Logger system health events related to EPS usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Network/
Elevated Threat Condition	This filter identifies events with a Priority level rating of 5 or 6.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
FAN Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is FAN for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/
Green Threshold	This filter selects that event remaining count in message bus is less than certain time events, by default, it is 10 minutes.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Guarded Threat Condition	This filter identifies events with a Priority level rating of 3 or 4.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
High Threat Condition	This filter identifies events with a Priority level rating of 7 or 8.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Hour less than 10	This filter is used by a Conditional DV. The condition in the filter is Hour(EndTime) is less than 10.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
Logger Application Events	This filter identifies Logger application events.	/All Filters/ArcSight Administration/Logger/Event Types/
Logger Disk Usage	This filter detects Logger system health events related to remaining disk space.	/All Filters/ArcSight Administration/Logger/ArcSight Appliances Overview/

Filter Resources, continued

Resource	Description	URI
Logger Events	This filter identifies Logger events.	/All Filters/ArcSight Administration/Logger/Event Types/
Logger Hardware Status	This filter identifies ArcSight correlation events that are generated by the Logger Status rule or by the Logger Sensor Status rule and where the sensor status (device custom string 3) is not OK.	/All Filters/ArcSight Administration/Logger/ArcSight Appliances Overview/
Logger Platform Events	This filter identifies Logger platform events.	/All Filters/ArcSight Administration/Logger/Event Types/
Logger System Health Events	This filter identifies Logger system health events.	/ArcSight Administration/Logger/Event Types/
Low Threat Condition	This filter identifies events with a Priority level rating less than or equal to 2.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
Memory Usage	This filter identifies Logger system health events related to memory usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/CPU and Memory/
Message Bus Status Events	This filter selects status audit events for message bus.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Message Count Remaining in Message Bus	This filter selects audit events for messages remaining in message bus.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Minute less than 10	This filter is used by a Conditional DV. The condition in the filter is Minute(EndTime) is less than 10.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/Conditional Variable Filters/
My Logger	This filter is used by all the My Logger dashboards and data monitors. The filter defines conditions to select one Logger to be used by these dashboards and data monitors. The default value is 127.0.0.1. Edit the IP address to match your Logger. Note: Only monitor one Logger at a time.	/All Filters/ArcSight Administration/Logger/System Health/
Network Usage	This filter identifies Logger system health events related to network usage that originate from the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Network/

Filter Resources, continued

Resource	Description	URI
Notification Actions	This filter selects events that are related to notifications generated by a rule in the ArcSight ESM system.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Flow/
Red Threshold	This filter selects that event remaining count in message bus exceeds certain time events, by default, it is one hour.	/All Filters/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Resource Changes	This filter detects resource change audit events.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Deletes	This filter detects deleted resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Inserts	This filter detects new resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Resource Updates	This filter detects updates to resources.	/All Filters/ArcSight Administration/ESM/Configuration Changes/Resource Update Tracking/
Rules Engine Internal Events	This filter identifies internal ArcSight ESM rules engine base events.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Rules/
Sensor Type Update	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Type Status rule or by the Logger Sensor Status rule and where the sensor status (device custom string 3) is not OK for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/
Severe Threat Condition	This filter identifies events with Priority level rating greater than 8.	/All Filters/ArcSight Administration/ESM/System Health/Events/Event Priority Filters/
System Sensors	This filter identifies ArcSight correlation events that are generated by the Logger Sensor Status rule and where the sensor type (device custom string 4) is not CPU or FAN for the Logger defined in the My Logger filter.	/All Filters/ArcSight Administration/Logger/System Health/Hardware/Sensors/

Filter Resources, continued

Resource	Description	URI
Threshold - Critical	This filter is used in the ASM Database Free Space - Critical rule. The filter identifies events in which the free space is less than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/ESM/System Health/Storage/Custom/
Threshold - Warning	This filter is used in the ASM Database Free Space - Warning rule. The filter captures events where the free space is less than or equal to five percent, but more than two percent. The audit event uses Device Custom Number1 to report the database free space.	/All Filters/ArcSight Administration/ESM/System Health/Storage/Custom/
Trend Query Returning No Results	This filter detects successful trend query events that return no results.	/All Filters/ArcSight Administration/ESM/System Health/Resources/Trends/

Global Variables

The following table lists all the global variables.

Global Variable Resources

Resource	Description	URI
Actor	This field returns the actor name.	/All Global Variables/ArcSight Administration/ESM/Actor/
ActorFromFileName	This global variable selects the actor based on the value in the file name and is used with actor audit events.	/All Global Variables/ArcSight Administration/ESM/Actor/
All Receivers and Forwarders	This field shows the EPS from all connector and forwarder agents connected to this ArcSight ESM.	/All Global Variables/ArcSight Administration/Logger/
CPU Name	The field returns the name of the CPU currently used.	/All Global Variables/ArcSight Administration/Logger/
Change Source	This field returns the source of the change that modified the actor resource.	/All Global Variables/ArcSight Administration/ESM/Actor/
ConnectorID	This variable returns the Resource ID of the connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/

Global Variable Resources, continued

Resource	Description	URI
ConnectorName	This variable returns the name of the connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/
ConnectorNameFromID	This variable returns the name of the Connector by looking up the Connector ID in the Connector Information Active List.	/All Global Variables/ArcSight Administration/ESM/Licensing/
ConnectorType	This variable returns the type of connector.	/All Global Variables/ArcSight Administration/ESM/Licensing/
DN New Value	This global variable extracts the new value for DN (Distinguished Name) in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
DN Old Value	This global variable extracts the old value for DN (Distinguished Name) in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Department New Value	This global variable extracts the new value for Department in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Department Old Value	This global variable extracts the old value for Department in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Disk Name	This field returns the name of the disk currently being used.	/All Global Variables/ArcSight Administration/Logger/
Disk Usage	This field returns the disk usage status whether it is normal or nearing critical usage (less than ten percent).	/All Global Variables/ArcSight Administration/Logger/
DiskUsageCritical	This field returns a value of Critical if the disk usage is determined to be less than five percent. If not, a value of Warning is returned.	/All Global Variables/ArcSight Administration/Logger/
Email Address New Value	This global variable extracts the new value for Email Address in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Email Address Old Value	This global variable extracts the old value for Email Address in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Employee Type New Value	This global variable extracts the new value for the Employee Type in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/

Global Variable Resources, continued

Resource	Description	URI
Employee Type Old Value	This global variable extracts the old value for Employee Type in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Field Status	This field is an alias field for Device Custom String3.	/All Global Variables/ArcSight Administration/Logger/
Field Value	This field is an alias field for Device Custom Number1.	/All Global Variables/ArcSight Administration/Logger/
Free Space	This field is an alias field for Device Custom Number1.	/All Global Variables/ArcSight Administration/Logger/
Full Name New Value	This global variable extracts the new value for Full Name in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Full Name Old Value	This global variable extracts the old value for Full Name in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Inbound and Outbound	This field returns a value of Inbound or Outbound via a filter that determines whether an event is an inbound or an outbound event.	/All Global Variables/ArcSight Administration/Logger/
IndexOfUsage	This field returns the index position of the string /Usage within the Device Event Category field.	/All Global Variables/ArcSight Administration/Logger/
Location New Value	This global variable extracts the new value for Location in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Location Old Value	This global variable extracts the old value for Location in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Logger Address	This field is an alias to the Device Address field.	/All Global Variables/ArcSight Administration/Logger/
Logger IP	This field is an alias to Destination Translated Address.	/All Global Variables/ArcSight Administration/Logger/
Manager New Value	This global variable extracts the new value for Manager in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/

Global Variable Resources, continued

Resource	Description	URI
Manager Old Value	This global variable extracts the old value for Manager in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Memory Name	This field returns a memory related value located within the Device Event Category field.	/All Global Variables/ArcSight Administration/Logger/
Org New Value	This global variable extracts the new value for Org in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Org Old Value	This global variable extracts the old value for Org in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
ReadOrWrite	This field returns whether the logger event is a read or write event.	/All Global Variables/ArcSight Administration/Logger/
Sensor Name	This field is an alias for Device Custom String5.	/All Global Variables/ArcSight Administration/Logger/
Sensor Status	This field is an alias for Device Custom String3.	/All Global Variables/ArcSight Administration/Logger/
Sensor Type	This field is an alias for Device Custom String4.	/All Global Variables/ArcSight Administration/Logger/
Status New Value	This global variable extracts the new value for Status in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Status Old Value	This global variable extracts the old value for Status in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Timeframe	This field is an alias for Device Custom String2.	/All Global Variables/ArcSight Administration/Logger/

Global Variable Resources, continued

Resource	Description	URI
Title New Value	This global variable extracts the new value for Title in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Title Old Value	This global variable extracts the old value for Title in actor update audit events (single-value parameters).	/All Global Variables/ArcSight Administration/ESM/Actor/
Unit	This field is an alias for Device Custom String1.	/All Global Variables/ArcSight Administration/Logger/

Integration Commands

The following table lists all the integration commands.

Integration Command Resources

Resource	Description	URI
By Destination	This integration command enables you to run a search by destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Event Name	This integration command enables you to run a search by event name on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Source	This integration command enables you to run a search by source address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By Source and Destination	This integration command enables you to run a search by source and destination address on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
By User	This integration command enables you to run a search by user on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	All Integration Commands/ArcSight Administration/Logger/
By Vendor and Product	This integration command enables you to run a search by device vendor and product on an ArcSight Logger appliance. The search returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/
Logger Quick Search	This integration command enables you to run a search on an ArcSight Logger appliance. The search takes the selected field type and value as parameters, and returns all the events matching the condition within the last two hours.	/All Integration Commands/ArcSight Administration/Logger/

Integration Configurations

The following table lists all the integration configurations.

Integration Configuration Resources

Resource	Description	URI
ArcSight Investigate Search	This integration configuration is used to configure the ArcSight Investigate search commands.	/All Integration Configurations/ArcSight Administration/ArcSight Investigate/
Logger Quick Search	This integration configuration is used to configure the Logger Quick Search command.	/All Integration Configurations/ArcSight Administration/Logger/
Logger Search	This integration configuration is used to configure the Logger Search command.	/All Integration Configurations/ArcSight Administration/Logger/

Integration Targets

The following table lists all the integration targets.

Integration Target Resources

Resource	Description	URI
ArcSight Investigate 1	This integration target stores the hostname and port number of an ArcSight Investigate. This target is used by the set of integration commands for ArcSight Investigate search.	/All Integration Targets/ArcSight Administration/ArcSight Investigate/
Logger Appliance 1	This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger.	/All Integration Targets/ArcSight Administration/Logger/
Logger Appliance 2	This integration target stores the IP address of an ArcSight Logger appliance. This target is used by the set of integration commands for Logger.	/All Integration Targets/ArcSight Administration/Logger/

Queries

The following table lists all the queries.

Query Resources

Resource	Description	URI
ASM Database Free Space	This query looks for internal events showing free space percentage for ASM database table spaces. The query returns the table spaces and free space percentages. The query is used by the ASM Database Free Space trend.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Event Queries/
ASM Database Free Space (current)	This query looks for internal events showing free space percentage for ASM database table spaces. The query returns one table space and its free space percentage using the device event category field as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/
ASM Database Free Space - by Day	This query on the ASM Database Free Space trend returns the day and minimum free space percentage for one of the ASM database table spaces using the TableName variable as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Trend Queries/
ASM Database Free Space - by Hour	This query on the ASM Database Free Space trend returns the hour and free space percentage for one of the ASM database table spaces using the TableName variable as a parameter.	/All Queries/ArcSight Administration/ESM/System Health/Storage/Trend Queries/
Active List Access	This query retrieves the number of times active lists are accessed (addition, deletion, and update of active list entries) in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Active List Access (Details)	This query retrieves details about the active lists that are accessed (addition, deletion, and update of active list entries) per active list by ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Actor Authenticators	This query identifies all the authenticators for actors.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Configuration Changes	This query identifies all configuration change audit events made to actor resources. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/

Query Resources, continued

Resource	Description	URI
Actor Full Name and Email Changes	This query identifies information from actor audit events that result from changes to the Full Name or Email attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Manager and Department Changes	This query identifies information from actor audit events that result from changes to the Department or Manager attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Title and Status Changes	This query identifies information from actor audit events that result from changes to the Title or Status attribute of an actor. This query shows the old and the new information.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Created	This query identifies audit events for actors that have been created. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Deleted	This query identifies audit events for actors that have been deleted. Note: This query does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Actors Updated	This query identifies audit events for actors that have been updated. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
All Devices Detected Inactive - Last 24 Hours	This query retrieves devices detected as inactive within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Devices Detected Inactive - Last 7 Days	This query retrieves devices detected as inactive within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This query retrieves devices from the All Monitored Devices active list.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Green	This query retrieves devices detected as active within the last 20 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/

Query Resources, continued

Resource	Description	URI
All Monitored Devices - Green Counter	This query retrieves devices detected as active within the last 20 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Red	This query retrieves devices detected as inactive for more than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Red Counter	This query retrieves devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Yellow	This query retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices - Yellow Counter	This query retrieves devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
ArcSight User Hourly Login Trends	This query on the ArcSight User Login Trends - Hourly trend selects the Target User Name, Attacker Zone, Attacker Address, and the Hour of each Console login for the ArcSight User Login Trends report.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Logins - Last Hour	This query selects events matching the ArcSight Login Rule Firings filter, collecting the Attacker Address, Attacker Asset Name, Attacker Zone, Device Event Category, End Time, Target User Name, and the LoginHour (a variable based on the End Time). This query is used to populate the ArcSight User Login Trends - Hourly trend.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
Average Data Monitor Evaluations Per Second	This query identifies the average number of data monitor evaluations per second in ten minute intervals for the last hour.	ArcSight Administration/ESM/System Health/Resources/Data Monitors/
Breakdown by Device Address From Connector	This query selects the top 20 devices within the last 24 hours by connector.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Device Address From Vendor and Product	This query selects the top 20 devices within the last 24 hours by the vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/

Query Resources, continued

Resource	Description	URI
Breakdown by Event Names From Connector	This query selects the top 20 event names within the last 24 hours by connector.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Names From Device	This query selects the top 20 event names within the last 24 hours by device.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Names From Vendor and Product	This query selects the top 20 event names within the last 24 hours by the vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Event Name/
Breakdown by Event Priority From Connector	This query selects the event priority within the last 24 hours by connector.	ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Device	This query selects the event priority within the last 24 hours by device.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Vendor and Product	This query selects the events priority within the last 24 hours by vendor and product.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Cache History by Connectors	This query identifies the cache history for one connector (using a parameter) in the Connector - Caches session list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connector Average EPS - Last 7 Days	This query identifies the average EPS for all connectors during the last seven days from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Daily Average EPS	This query identifies the daily average EPS for all connectors from a trend. It is used to build a trend-on-trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Monitor Event	This query identifies the total number of events that connectors forward to the ArcSight Manager per hour.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Connector Severity Hourly Stacked Chart	This query replaces the Agent Severity Hourly Stacked Chart Query.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Connector Upgrades Count	This query identifies the count of successful and failed connector upgrades per day in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Upgrades Count (Total)	This query identifies the total count of successful and failed connector upgrades in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions	This query identifies all the connectors with their latest versions in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Connector Versions by Type	This query identifies all the connectors with their latest versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Connectors - Caching - Long Term	This query identifies data on connectors that have been caching for more than two hours (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Caching - Short Term	This query identifies data on connectors that have been caching for under two hours (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Down	This query identifies data on connectors that have been down for under 20 minutes (by default). The queries are used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/
Connectors - Dropping Events	This query identifies data on connectors that have filled their caches to the point that they are dropping events. The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Connectors - Still Down	This query identifies data on connectors that have been down for longer than 20 minutes (by default). The query is used on an active list that is maintained by the Connector Monitoring content (rules).	/All Queries/ArcSight Administration/Connectors/System Health/Connector Monitoring/
Correlation Events Count	This query retrieves the total number of correlation events within the last hour, grouping them by ten minute intervals.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/

Query Resources, continued

Resource	Description	URI
Correlation Events Count (Details)	This query retrieves the number of correlation events per rule within the last hour, grouping them by ten minute intervals.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/
Critical Devices Detected Inactive - Last 24 Hours	This query retrieves critical devices detected as inactive within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Devices Detected Inactive - Last 7 Days	This query retrieves critical devices detected as inactive within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices	This query retrieves critical devices from the Critical Monitored Devices active list.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Green	This query retrieves critical devices detected as active within the last 20 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Green Counter	This query retrieves critical devices detected as active within the last 20 minutes and sorts them by product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Red	This query retrieves critical devices detected as inactive for more than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Red Counter	This query retrieves critical devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Yellow	This query retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices - Yellow Counter	This query retrieves critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/

Query Resources, continued

Resource	Description	URI
Current Cache Status - Caching Events	This query identifies the connectors in the Connectors - Caching session list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Current Cache Status - Dropping Events	This query identifies the connectors in the Connectors - Dropping Events active list.	/All Queries/ArcSight Administration/Connectors/System Health/Cache/
Destination Counts	This query retrieves destination details and the sum of event counts for each destination.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Destination Counts by Connector Type	This query identifies the Agent Type (Connector), Target Zone Name and Target Address, and a count of these events, sorted by Agent Type. The events are not restricted by any filtering conditions.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
ESM Configuration Changes	This query identifies all the successful configuration changes made to ArcSight ESM. The query identifies the name, the user, the device, and the time the change was made.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
EPS Received in Correlator	This query retrieves EPS count for events received in correlator.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Event Count by Agent Severity	This query retrieves events by agent severity with event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Event Count by Source Destination Pairs	This query retrieves event counts ordered by source-destination pairs.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Event Details	This query selects the End Time, Name, Attacker Address, Target Address, Device Address, Device Product, Device Vendor, Priority, Event ID, Device Zone Name, and the local variables Device Information, Vendor and Product, Connector Information.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Event Distribution Chart for a Connector Type	This query retrieves the hourly distribution of events for a specific connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Event Name Counts	This query retrieves the event names and their event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Events Count	This query selects the sum of the Aggregated Event Count for non-ArcSight events. The query is used by the Events Count trend.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 30 Days	This query on the Events Count trend selects the total number of non-ArcSight events within the last 30 days.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 7 Days	This query on the Events Count trend selects the total number of non-ArcSight events and the time stamp within the last seven days.	/All Queries/ArcSight Administration/ESM/Event Analysis Overview/
Events by ArcSight Priority (Summary)	This query identifies the ArcSight Priority, event Name, and the sum of the Aggregated Event Count for all events used in the Events by ArcSight Priority (Summary) report.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Events by Connector Type (Summary)	This query retrieves details about various connectors and event counts for each connector.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Device (Summary)	This query retrieves the various devices and event counts for each device.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Selected Connector Type	This query retrieves events and their counts for a specific connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events for a Destination by Connector Type	This query identifies the Priority, End Time, Agent Type, Attacker Zone Name, Attacker Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time (hour). The events selected are from the Target Zone and Target Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values, either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/

Query Resources, continued

Resource	Description	URI
Events from a Source by Connector Type	This query identifies the Priority, End Time, Agent Type, Target Zone Name, Target Address, event Name, and the sum of the Aggregated Event Count, ordered by descending priority and by time. The events selected are from the Attacker Zone and Attacker Address fields, which default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values either in the Parameters tab of the report or manually when running the report. The Attacker and Target fields are used instead of Source and Destination fields.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Failed Connector Upgrades	This query identifies the connectors with failed upgrades (and the reason for the failure) in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Failed Queries	This query identifies failed queries for reports, trends, and query viewers. The query is used to build a trend and a query viewer.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Failed Queries - Trend	This query retrieves failed queries for reports, trends, and query viewers from a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/
High Volume Connector EPS - By Day	This query identifies the daily average EPS for high volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
High Volume Connector EPS - Hourly	This query identifies the hourly average EPS for high volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Hourly Distribution Chart for Event	This query retrieves the hourly distribution of specific events.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Distribution Chart for a Destination Port	This query retrieves the hourly distribution of events for destinations with a specific port.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

Query Resources, continued

Resource	Description	URI
Hourly Distribution Chart for a Source Port	This query retrieves the hourly distribution of events for sources with a specific port.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly EPS in Persistor	This query selects hourly EPS in persistor.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Hourly Event Counts (Area Chart)	This query retrieves the hourly distribution of event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This query retrieves the hourly distribution of events by priority rating.	/All Queries/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
IDM Deletions of Actors	This query identifies information about actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Actors/
Invalid Resources	This query retrieves a list of invalid resources from the Invalid Resources active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/
Invalid Resources (Chart)	This query retrieves the count of invalid resources by resource type from the Invalid Resources active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/
Last 10 QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Last 10 Report Queries	This query retrieves report query duration information, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Last 10 Trend Queries	This query retrieves trend query duration information, ordered by end time.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Licensing Query	This query retrieves the licensing history for the various license types taken from the License History session list.	/All Queries/ArcSight Administration/ESM/Licensing/

Query Resources, continued

Resource	Description	URI
Longest QueryViewer Queries	This query retrieves query duration information for query viewers, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Longest QueryViewer Queries - Trend	This query retrieves query viewer query duration information from trends, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Longest Report Queries	This query retrieves report query duration information, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Longest Report Queries - Trend	This query retrieves report query duration information from trends, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Longest Trend Queries	This query retrieves trend query duration information, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Longest Trend Queries - Trend	This query retrieves trend query duration information from a trend, ordered by duration.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Low Volume Connector EPS - By Day	This query defines the daily average EPS for low volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
Low Volume Connector EPS - Hourly	This query defines the hourly average EPS for low volume connectors from a trend.	/All Queries/ArcSight Administration/Connectors/System Health/EPS/
MPS Received in Aggregator	This query retrieves messages per second (MPS) count for events received in aggregator.	/All Queries/ArcSight Administration/ESM/Distributed Correlation Monitoring/
New Devices Detected - Last 24 Hours	This query retrieves all new devices detected within the last 24 hours.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
New Devices Detected - Last 7 Days	This query retrieves all new devices detected within the last seven days.	/All Queries/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Number of Events matching Rules	This query retrieves the total number of events matching rules (events matching filter rules, join rules, and the total of both types of rules) within the last hour grouping them by ten minute intervals.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/

Query Resources, continued

Resource	Description	URI
Query Counts During Last 24 hr	This query identifies the resource type and its counts from the Query Running Time active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
Query Counts During Last Week	This query retrieves resource types and their counts from the Query Running Time active list.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Queries/
QueryViewer Failures	This query retrieves query duration information for failed query viewers.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
QueryViewer Queries	This query retrieves query duration information for query viewers used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/QueryViewers/
Report Queries	This query retrieves report query duration information used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Report Query Failures	This query retrieves failed query duration information for reports.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Resource Created Report	This query identifies all the resources that have been created by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Deleted Report	This query identifies all the resources that have been deleted by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource History Report	This query identifies all the resources that have been created, updated, or deleted by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Updated Report	This query identifies all the resources that have been updated by ArcSight users. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Queries/ArcSight Administration/ESM/Configuration Changes/Resources/
Rules Engine Warning Messages	This query retrieves warning messages received from the rules engine.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Rules/
Running Report Queries	This query retrieves currently running report queries.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/

Query Resources, continued

Resource	Description	URI
Running Trend Queries	This query retrieves running trend query duration information.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Session List Access	This query retrieves the number of times session lists are accessed (addition, deletion, and update of session list entries) in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Session List Access (Details)	This query retrieves details of session list access (addition, deletion, and update of active list entries) per session list in ten minute intervals for the last hour.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Source Counts by Connector Type	This query identifies the Agent Type (Connector), Attacker Zone Name and Attacker Address, and a count of these events, sorted by Agent Type. The events are not restricted by any filtering conditions.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Source Counts by Event Name	This query retrieves event names by source address in addition to event counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/
Storage Licensing Data	This query selects the raw event length for each day for all the connectors from an active list.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data - trend	This query selects the raw event length for each day for all the connectors from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data by Connector Name - trend	This query selects the raw event length by connector name for each day from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Storage Licensing Data by Connector Type - trend	This query selects the raw event length by connector type for each day from a trend.	/All Queries/ArcSight Administration/ESM/Licensing/
Successful Connector Upgrades	This query identifies the connectors with successful upgrades (and the new connector version) in the Connectors Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Query Resources, continued

Resource	Description	URI
Top 10 Events	This query retrieves the top events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Inbound Events	This query retrieves the top inbound events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Outbound Events	This query retrieves the top outbound events ordered by their counts.	/All Queries/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top Accessed Active Lists	This query retrieves the most accessed active lists (addition, deletion, and update of active list entries) within the last hour and orders them by most accessed.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Top Accessed Session Lists	This query retrieves the most accessed session lists (addition, deletion, and update of session list entries) with in the last hour and orders them by most accessed.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Top Connector Types Chart	This query retrieves connector details with event counts for each connector type.	/All Queries/ArcSight Administration/Connectors/System Health/Event Breakdown/
Trend Query	This query retrieves trend query duration information used to build a trend.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Trend Query Failures	This query retrieves failed trend query duration information.	/All Queries/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Upgrade History by Connector	This query identifies all the connector upgrades (successful and failed) by connector in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Upgrade History by Connector Type	This query identifies all the connector upgrades (successful and failed) by connector type in the Connector Upgrades active list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Upgrades/

Query Resources, continued

Resource	Description	URI
User Login Logout Report	This query retrieves user login (success/fail) and logout events.	/All Queries/ArcSight Administration/ESM/User Access/User Sessions/
Version History by Connector	This query identifies all the connector versions by connector in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/
Version History by Connector Type	This query identifies all the connectors and connector versions by connector type in the Connector Versions session list.	/All Queries/ArcSight Administration/Connectors/Configuration Changes/Versions/

Query Viewers

The following table lists all the query viewers.

Query Viewer Resources

Resource	Description	URI
Active Critical Devices - last 20 min	This query viewer displays details for the critical devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Active Critical Devices by Product - last 20 min	This query viewer displays details for the critical devices detected as active for the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Active Devices - last 20 min	This query viewer displays details for the devices detected as active for the last 20 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Active Devices by Product - last 20 min	This query viewer displays details for the devices detected as active within the last 20 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Actor Authenticators	This query viewer displays a list of all the authenticators for actors.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Configuration Changes	This query viewer displays all audit events that result from changes to actor resources. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/

Query Viewer Resources, continued

Resource	Description	URI
Actor Full Name and Email Changes	This query viewer displays information from actor audit events that result from changes to the Full Name or Email attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Manager and Department Changes	This query viewer displays information from actor audit events that result from changes to the Department or Manager attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actor Title and Status Changes	This query viewer displays information from actor audit events that result from changes to the Title or Status attribute of an actor. This query viewer shows the old and the new information.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Created	This query viewer displays all the audit events for actors that have been created. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Deleted	This query viewer displays audit events for actors that have been deleted. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Actors Updated	This query viewer displays audit events for actors that have been updated. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
All Monitored Devices	This query viewer displays details for the devices detected within the last 365 days.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Breakdown by Device Address From Connector	This query viewer shows the top 20 devices within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Device Address From Vendor and Product	This query viewer shows the top 20 devices within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Device Address/
Breakdown by Event Names From Connector	This query viewer shows the top 20 event names within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/

Query Viewer Resources, continued

Resource	Description	URI
Breakdown by Event Names From Device	This query viewer shows the top 20 event names within the last 24 hours by device.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/
Breakdown by Event Names From Vendor and Product	This query viewer shows the top 20 event names within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Name/
Breakdown by Event Priority From Connector	This query viewer shows the event priority within the last 24 hours by connector.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Device	This query viewer shows the event priority within the last 24 hours by device.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Breakdown by Event Priority From Vendor and Product	This query viewer shows the event priority within the last 24 hours by vendor and product.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/by Priority/
Connectors - Caching - Long Term	This query viewer displays data on connectors that have been caching for more than two hours (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Caching - Short Term	This query viewer displays data on connectors that have been caching for under two hours (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Down - Long Term	This query viewer displays data on connectors that have been down for longer than 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Connectors - Down - Short Term	This query viewer displays data on connectors that have been down for under 20 minutes (by default). This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/

Query Viewer Resources, continued

Resource	Description	URI
Connectors - Dropping Events	This query viewer displays data on connectors that have filled their caches to the point that they are dropping events. This query viewer queries on an active list that is maintained by the Connector Monitoring content (rules), so it can update every minute.	/All Query Viewers/ArcSight Administration/Connectors/System Health/
Critical Monitored Devices	This query viewer displays details for all critical devices.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Event Details	This query viewer shows the event details.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 30 Days	This query viewer shows the total number of non-ArcSight events within the last 30 days.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Events Count Last 7 Days	This query viewer shows the total number of non-ArcSight events each day for the last seven days.	/All Query Viewers/ArcSight Administration/ESM/Event Analysis Overview/
Hourly EPS Received in Correlator	This query viewer displays hourly EPS received in correlator.	/All Query Viewers/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Hourly Messages Per Second Received in Aggregator	This query viewer displays hourly messages per second received in aggregator.	/All Query Viewers/ArcSight Administration/ESM/Distributed Correlation Monitoring/
IDM Deletions of Actors	This query viewer displays information about actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system. Note: This query viewer does not populate all values when running in Turbo Mode Fastest.	/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/
Inactive Critical Devices - more than 20 min	This query viewer displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Critical Devices - more than 60 min	This query viewer displays details for the critical devices detected as inactive for more than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/

Query Viewer Resources, continued

Resource	Description	URI
Inactive Critical Devices by Product - more than 20 min	This query viewer displays details for the critical devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Critical Devices by Product - more than 60 min	This query viewer displays details for the critical devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Inactive Devices - more than 20 min	This query viewer displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices - more than 60 min	This query viewer displays details for the devices detected as inactive for more than 60 minutes.	ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices by Product - more than 20 min	This query viewer displays details for the devices detected as inactive for more than 20 minutes but less than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Inactive Devices by Product - more than 60 min	This query viewer displays details for the devices detected as inactive for more than 60 minutes and sorts them by device product.	/All Query Viewers/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Last 10 Query Viewer Queries	This query viewer shows the last ten query viewer query duration information.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Last 10 Report Queries	This query viewer shows the duration information for the last ten report queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Last 10 Trend Queries	This query viewer shows the duration information for the last ten trend queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Query Counts During Last 24 hr	This query viewer shows the query and its counts during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/
Query Failures During Last 24 hr	This query viewer displays failed queries for reports, trends, and query viewers.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/

Query Viewer Resources, continued

Resource	Description	URI
Query Viewer Failures During Last 24 hr	This query viewer shows the failed query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Report Query Failures During Last 24 hr	This query viewer shows the duration information for failed report queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Running Report Queries	This query viewer shows the currently running report queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Running Trend Queries	This query viewer shows the currently running trend queries.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Top 10 Longest Query Viewer Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest query viewers during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Query Viewers/
Top 10 Longest Report Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest report queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Reports/
Top 10 longest Trend Queries During Last 24 hr	This query viewer shows the duration information for the top ten longest trend queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/
Trend Queries Failures During Last 24 hr	This query viewer shows the duration information for failed trend queries during the last 24 hours.	/All Query Viewers/ArcSight Administration/ESM/System Health/Resources/Reporting/Trends/

Reports

The following table lists all the reports.

Report Resources

Resource	Description	URI
Active List Access	This report shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries within the previous day, grouping the counts by ten minute intervals. A table shows the details of the active list access, grouping the number by time interval and active list name.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Active Lists/
Actor Full Name and Email Changes	This report shows information from actor audit events that result from changes to the Full Name or Email attribute of an actor. The report shows the old and new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Manager and Department Changes	This report shows information from actor audit events that result from changes to the Department or Manager attribute of an actor. This report shows the old and the new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Actor Title and Status Changes	This report shows information from actor audit events that result from changes to the Title or Status attribute of an actor. The report shows the old and new information.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
All Devices Detected Inactive - Last 24 Hours	This report shows all devices detected as inactive within the last 24 hours.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Devices Detected Inactive - Last 7 Days	This report shows all devices detected as inactive within the last seven days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
All Monitored Devices	This report shows all devices detected within the last 365 days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
ArcSight User Login Trends	This report shows a summary of the number of ArcSight user logins within the previous day. A bar chart shows the total number of logins by user and a table shows the number of logins by user per hour.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/

Report Resources, continued

Resource	Description	URI
ArcSight User Logins - Last Hour	This report shows details for all the ArcSight user logins within the past hour. The report contains a table showing the source host, the username, and the login time.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/
Cache History by Connectors	This report shows the cache history by connector (within the last 24 hours by default) sorted chronologically. Notes: When running this report, you can specify the Connector URI (located in the connector resource navigator or the Connector Information active list) in the ConnectorURI field in the custom parameters for the report. By default, the report shows all of the connectors known by the system. You can further specify the ConnectorURI parameter to narrow down the connector cache histories reported, from groups (such as /All Connectors/Site Connectors/) down to a specific connector (such as /All Connectors/Site Connectors/DMZ/WUC-1). The default time range of this report is the past three to four months.	/All Reports/ArcSight Administration/Connectors/System Health/Cache/
Configuration Changes by Type	This report shows recent actor configuration changes. A table lists all the changes grouped by type and user, and sorts them chronologically.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Configuration Changes by User	This report shows recent actor configuration changes. A table lists all the changes grouped by user and type, and sorts them chronologically.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Connector Severity Hourly Stacked Chart	This report shows hourly event count data ordered by severity in a stacked chart.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Connector Upgrades Count	This report shows the total count of successful and failed connector upgrades in a pie chart, and the counts per day in a table (within the last seven days by default).	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Connector Versions	This report lists all the connectors with their latest versions (within the last seven days by default). The list is grouped by connector type, connector zone, and connector address.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/

Report Resources, continued

Resource	Description	URI
Connector Versions by Type	This report lists all the connectors with their latest versions (within the last seven days by default). The list is grouped by connector version, connector zone, and connector address.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/
Correlation Events Statistics	This report shows correlation event statistics. A chart shows the number of correlation events within the last hour, grouping them by ten minute intervals. A table shows details of the number of correlation events, grouping them by rule name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/
Created	This report shows a list of all the actors created on the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Critical Devices Detected Inactive - Last 24 Hours	This report shows critical devices detected as inactive within the last 24 hours.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Devices Detected Inactive - Last 7 Days	This report shows critical devices detected as inactive within the last seven days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Critical Monitored Devices	This report shows all critical devices currently being monitored.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - Critical/
Current Cache Status	This report lists the connectors that are currently caching and dropping events. The first table shows the connectors that are dropping events. The second table shows the connectors that are caching.	/All Reports/ArcSight Administration/Connectors/System Health/Cache/
Data Monitor Evaluations Statistics	This report shows a chart with the average number of data monitor evaluations per second.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Data Monitors/
Deleted	This report displays audit event information for actors that have been deleted. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/

Report Resources, continued

Resource	Description	URI
Destination Counts	This report shows destination details and the sum of event counts for each destination.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Destination Counts by Connector Type	This report displays a table showing the connector type, the destination zones and addresses, and the count from each source. Make sure you select a filter parameter other than the default of All Events. You can also adjust the Start and End times of the report to reduce the number of events selected.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
ESM Configuration Changes by Type	This report shows recent ArcSight ESM configuration changes. A table lists all the changes, grouped by type and user, and sorts them chronologically. This report enables you to find all the configuration changes of a certain type quickly.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
ESM Configuration Changes by User	This report shows recent ArcSight ESM configuration changes. A table lists all the changes, grouped by user and type, and sorts them chronologically. This report enables you to find all the configuration changes made by a specific user.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
Event Count by Agent Severity	This report shows events by agent severity with event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Event Count by Source Destination Pairs	This report shows event counts ordered by source-destination pairs.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Event Distribution Chart for a Connector Type	This report shows the hourly distribution of events for a specific connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Event Name Counts	This report shows event names and their event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/

Report Resources, continued

Resource	Description	URI
Events by ArcSight Priority (Summary)	This report displays a table of all events, grouped by ArcSight Priority, showing the count of each event occurrence within that priority. Note: This report shows all ArcSight events; use the FilterBy parameter to limit the output to the areas of most interest.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Events by Connector Type (Summary)	This report shows events by connector type and the event counts for each connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Device (Summary)	This report shows various devices and event counts for each device.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events by Selected Connector Type	This report shows events and their counts for a specific connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events for a Destination by Connector Type	This report displays a table of all events showing time, source, and connector information based on the Target Zone and Target Address fields. These fields are used as the event destinations, and default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can change these default values either in the Parameters tab of the report or manually when running the report. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Events from a Source by Connector Type	This report displays a table of all events showing time, destination, and connector information based on the Attacker Zone and Attacker Address fields. These fields are used as the source of the events, and default to RFC1918: 192.168.0.0-192.168.255.255 and 192.168.10.10. You can be change these default values either in the Parameters tab of the report or manually when running the report.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/

Report Resources, continued

Resource	Description	URI
Failed Connector Upgrades	This report lists the connectors with failed upgrades (within the last seven days by default). The list is grouped by connector zone, connector address, connector name, and connector ID, and shows the reason for the failure.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Failed Queries	This report shows the failed queries for trend, report, and query viewers. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Fired Rule Events	This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/
High Volume Connector EPS - Daily	This report shows the hourly average EPS for high volume connectors. The default time frame is yesterday. By default, a connector with a daily average EPS greater than or equal to 100 is considered a high volume connector.	/All Reports/ArcSight Administration/Connectors/System Health/EPS/
High Volume Connector EPS - Weekly	This report shows the daily average EPS for high volume connectors. The default time frame is one week. By default, a connector with a daily average EPS greater than or equal to 100 is considered a high volume connector.	/All Reports/ArcSight Administration/Connectors/System Health/EPS/
Hourly Distribution Chart for Event	This report shows the hourly distribution of specific events.	/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Distribution Chart for a Destination Port	This report shows the hourly distribution of events for destinations with a specific port.	/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Distribution Chart for a Source Port	This report shows the hourly distribution of events for sources with a specific port.	/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
Hourly Event Counts (Area Chart)	This report shows the hourly distribution of event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/

Report Resources, continued

Resource	Description	URI
Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)	This report shows the hourly distribution of events by priority rating.	/All Reports/ArcSight Administration/ESM/System Health/Events/Time-Based Event Breakdowns/
IDM Deletions of Actors	This report shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Invalid Resources	This report shows a list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI.	/All Reports/ArcSight Administration/ESM/System Health/Resources/
Licensing Report	This report shows the licensing history for one of the license types. The chart shows the current count and the count limit in a chart. By default, the licensing history is over the last seven days.	/All Reports/ArcSight Administration/ESM/Licensing/
Licensing Report (All)	This report shows the licensing history for all the license types. The charts show the current count and the count limit for each of the license types. By default, the licensing history is over the last seven days.	/All Reports/ArcSight Administration/ESM/Licensing/
Longest QueryViewer Queries	This report shows query duration information for query viewers. A chart shows the top ten longest queries for a query viewer and a table shows the duration details for query viewers. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Longest Report Queries	This report shows query duration information for reports. The chart shows the top ten longest report queries and the table shows the duration details for the report queries. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/
Longest Trend Query	This report shows query duration information for trends. A chart shows the top ten longest trend queries and a table shows the duration details for trend queries. The default time frame is one week.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Reporting/

Report Resources, continued

Resource	Description	URI
Low Volume Connector EPS - Daily	This report shows the hourly average EPS for low volume connectors. The default time frame is yesterday. By default, a connector with a daily average EPS less than 100 is considered a low volume connector.	/All Reports/ArcSight Administration/Connectors/System Health/EPS/
Low Volume Connector EPS - Weekly	This report shows the daily average EPS for low volume connectors. The default time frame is one week. By default, a connector with a daily average EPS less than 100 is considered a low volume connector.	/All Reports/ArcSight Administration/Connectors/System Health/EPS/
New Devices Detected - Last 24 Hours	This report shows new devices detected within the last 24 hours.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
New Devices Detected - Last 7 Days	This report shows new devices detected within the last seven days.	/All Reports/ArcSight Administration/Devices/ArcSight ESM Device Monitoring - All/
Number of Events Matching Rules	This report shows the total number of events matching rules within the last hour, grouping them by ten minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both types of rules.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/
Query Counts by Type	This report shows query counts grouped by type. The default time frame is one week.	/ArcSight Administration/ESM/System Health/Resources/Reporting/
Resource Created Report	This report shows a list of all the resources created by ArcSight users in the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Deleted Report	This report shows a list of all the resources deleted by ArcSight users during the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource History Report	This report shows a list of all the resources that have been created, updated, or deleted by ArcSight users within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/
Resource Updated Report	This report shows a list of all the resources updated by ArcSight users within the previous day. Note: This report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Resources/

Report Resources, continued

Resource	Description	URI
Rules Engine Warning Messages	This report shows warning messages received from the rules engine.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Rules/
Session List Access	This report shows session list access statistics. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by 10 minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Source Counts by Connector Type	This report shows the connector type, the source zones and IP addresses, and the count from each source within the specified time period. Make sure that a filter parameter other than the default of All Events is selected. You can also adjust the start and end times of the report to reduce the number of events selected.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Source Counts by Event Name	This report shows event names by source address in addition to event counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/
Storage Licensing Report	This report shows an overview of the storage used by the system for each day, with a breakdown of the raw event data size sent by each connector and by connector type.	/All Reports/ArcSight Administration/ESM/Licensing/
Successful Connector Upgrades	This report lists the connectors with successful upgrades (within the last seven days by default). The list is sorted chronologically.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Top 10 Events	This report shows the top events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Inbound Events	This report shows the top inbound events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top 10 Outbound Events	This report shows the top outbound events ordered by their counts.	/All Reports/ArcSight Administration/ESM/System Health/Events/Top N Activity Reports/
Top Accessed Active Lists	This report shows the top ten accessed active lists. A chart shows the top ten accessed active lists in the previous day, grouping the counts by ten minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Active Lists/

Report Resources, continued

Resource	Description	URI
Top Accessed Session Lists	This report shows the top ten accessed session lists. A chart shows the top ten accessed session lists within the last hour, grouping the counts by ten minute intervals. A table shows details of the session list access, grouping the number by active list name and time interval.	/All Reports/ArcSight Administration/ESM/System Health/Resources/Session Lists/
Top Connector Types Chart	This report shows connector details with event counts for each connector type.	/All Reports/ArcSight Administration/Connectors/System Health/Event Breakdown/
Updated	This report shows a list of all the actors updated on the previous day. Note: This Report does not populate all values when running in Turbo Mode Fastest.	/All Reports/ArcSight Administration/ESM/Configuration Changes/Actors/
Upgrade History by Connector	This report shows the upgrade history by connector (within the last seven days by default) sorted chronologically. Note: When running the report, be sure to use the connector ID located in the connector resource and copy-paste the ID in to the ConnectorID field in the Custom Parameters for the report.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
Upgrade History by Connector Type	This report shows the upgrade history by connector type (within the last seven days by default). The report is grouped by connector zone, connector address, connector name, and connector ID.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Upgrades/
User Login Logout Report	This report shows user login events (success and fail) and logout events.	/All Reports/ArcSight Administration/ESM/User Access/User Sessions/

Report Resources, continued

Resource	Description	URI
Version History by Connector	This report shows the version history by connector (within the last seven days by default) sorted chronologically. Note: When running the report, use the connector ID (located in the connector resource) and copy-paste it in to the ConnectorID field in the Custom Parameters for the report.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/
Version History by Connector Type	This report shows the version history by connector type (within the last seven days by default). The list is grouped by connector zone, connector address, connector name, and connector ID.	/All Reports/ArcSight Administration/Connectors/Configuration Changes/Versions/
Web Users Licensing Report	This report shows the licensing history for web users. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.	/ArcSight Administration/ESM/Licensing/

Report Templates

The following table lists all the report templates.

Report Template Resources

Resource	Description	URI
Licensing Report	This report template is used by the licensing reports and shows one chart (bar and line). The orientation is landscape.	/All Report Templates/ArcSight Administration/Licensing/
Licensing Report (All)	This report template is used by the licensing reports and shows several charts (bar and line). The orientation is portrait.	/All Report Templates/ArcSight Administration/Licensing/

Rules

The following table lists all the rules.

Rule Resources

Resource	Description	URI
ASM Database Free Space - Critical	This rule detects internal events showing that one (or more) of the ASM database table spaces has a very low free space percentage. This is considered critical when the free space goes below the threshold defined in the server.properties file (two percent by default). A notification is sent to the Database Storage Operator group.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Free Space - Warning	This rule detects internal events showing that one (or more) of the ASM database table spaces has a low free space percentage. This is considered a warning when the free space goes below the threshold defined in the server.properties file (five percent by default).	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Critical	This rule detects if the database status is critical. This rule detects the insert and retrieval time for an event; the status is considered critical when the EventInsertTimeNanos field is greater than or equal to 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to very high.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Down	This rule detects if the database status is down. This rule detects the insert and retrieval time for an event; the status is considered down when the EventInsertTimeNanos field is equal to zero. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to unknown.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Normal	This rule detects if the database status is normal. This rule detects the insert and retrieval time of the event; the status is considered normal when the EventInsertTimeNanos (insert time in nanoseconds) field is less than or equal to 20,000. This rule requires two such events within two minutes. After the first event, the agentSeverity event field is set to low.	/All Rules/ArcSight Administration/ESM/System Health/Storage/

Rule Resources, continued

Resource	Description	URI
ASM Database Status Change - Space Critical	This rule detects if the database status is critical due to storage concerns. This rule detects a base event indicating that the database storage space is low. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to very high.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Space Now Available	This rule detects if the database status has returned to normal because storage space has been freed or added. This rule detects a base event indicating that database storage space is available. This rule only requires one such event to trigger. After the first event, the agentSeverity event field is set to Low.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
ASM Database Status Change - Warning	This rule detects if the database status is at a warning level. This rule detects the insert and retrieval time for an event; the status is considered a warning when the EventInsertTimeNanos field is between 20,000 and 50,000. This rule requires two such events within three minutes. After the first event, the agentSeverity event field is set to medium.	/All Rules/ArcSight Administration/ESM/System Health/Storage/
Alert - Critical Devices inactive for more than 1 hour	This rule triggers when a Connector Device Status event for critical devices has a zero in Device Custom Number2 and a Device Custom Date earlier than 60 minutes ago, which indicates that the device has been inactive for more than one hour. After the rule triggers, a notification is sent to the Device Administrators.	/All Rules/ArcSight Administration/Devices/
All Monitored Devices	This rule triggers when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check). After the rule triggers, the entry is created or updated in the All Monitored Devices active list.	/All Rules/ArcSight Administration/Devices/
ArcSight User Login	This rule detects ArcSight user login events. This rule adds the user information to the ArcSight User Sessions session list.	/All Rules/ArcSight Administration/ESM/User Access/User Sessions/
ArcSight User Login Timeout	This rule detects ArcSight user login timeout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user login timeout occurs.	/All Rules/ArcSight Administration/ESM/User Access/User Sessions/

Rule Resources, continued

Resource	Description	URI
ArcSight User Logout	This rule detects ArcSight user logout events. This rule terminates the ArcSight user session in the ArcSight User Sessions session list when an ArcSight user logout occurs.	/All Rules/ArcSight Administration/ESM/User Access/User Sessions/
Connector Added to Black List	This rule monitors the Black List - Connectors active list for new connector information. When a connector is added to the black list, this rule updates the other Connector Monitoring active lists to remove that connector from the status displays.	/All Rules/ArcSight Administration/Connectors/System Health/Custom/
Connector Cache Empty	This rule triggers when there is a connector cache empty event. The rule removes the connector from the Connector Caching and Connector Dropping Events active lists, and terminates the entry in the Connector - Caches session list.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Caching	This rule triggers when there is a connector caching event. The rule adds the connector and cache related information to the Connector Caching active list and the Connector - Caches session list.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Deleted	This rule identifies connector deleted events that are sent when a connector is deleted from the resource tree. On the first event, the session for the corresponding connector is terminated in the Connector Versions session list, and the connector is also removed from the Connectors - Down active list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/
Connector Discovered or Updated	This rule detects new connectors reporting to ESM and adds them to active lists to be monitored. Device Event Class ID = agent:007 is related to Agent Registration events. Device Event Class ID = agent:030 is related to Agent Start events. Device Event Class ID = agent:031 is related to Agent Shutdown events. Device Event Class ID = agent:101 is related to Agent Connection events. Device Event Class ID = agent:103 is related to Agent Heartbeat Timeout events. These events contain the detailed information necessary to populate the Connectors active lists.	/All Rules/ArcSight Administration/Connectors/System Health/

Rule Resources, continued

Resource	Description	URI
Connector Down	This rule triggers when there is a connector shutdown or heartbeat timeout event (except for connectors listed in the Black List - Connectors filter). The rule adds connector information to the Connectors - Down active list.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Dropping Events	This rule triggers when there is a connector dropping events event. The rule adds the connector and cache related information to the Connector Dropping Events active list and the Connector - Caches session list. A case can be created and a notification can be sent to the SOC operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Still Caching	This rule triggers when the TTL (two hours by default) for an entry in the Connectors - Caching active list expires. It then puts the connector information into the Connectors - Still Caching active list, creates a case and sends a notification to SOC Operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Still Down	This rule triggers when the TTL (20 minutes by default) for an entry in the Connectors - Down active list expires. The rule then adds the connector information to the Connectors - Still Down active list, creates a case and sends a notification to SOC Operators. Note: The case creation and notification actions are disabled by default.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Up	This rule triggers when there is a connector started event (except for connectors that match the conditions in the Black List - Connectors filter). The rule removes the connector from the connector connection status active lists.	/All Rules/ArcSight Administration/Connectors/System Health/
Connector Upgrade Failed	This rule detects failed connector upgrades. On every event, the connector information is added to the Connector Upgrades active list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/
Connector Upgrade Successful	This rule detects successful connector upgrades. On every event, the connector information is added to the Connector Upgrades active list. A new session is created in the Connector Versions session list. Note: The Agent configuration updated events are removed to avoid duplicate entries in the active list and session list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/

Rule Resources, continued

Resource	Description	URI
Connector Version Detected	This rule detects connector start events. The rule triggers if the connector is not yet in the Connector Versions session list. On every event, a new session with the connector information is created in the Connector Versions session list.	/All Rules/ArcSight Administration/Connectors/Configuration Changes/
Critical Monitored Devices	This rule triggers when a Connector Device Status event has a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check) and if the device entry exists in the Critical Monitored Devices active list. After the rule triggers, the active list entry is updated.	/All Rules/ArcSight Administration/Devices/
Detect Event Counts for Persistor	This rule populates the event counts for distributed correlation to a list.	/All Rules/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Detect Events for Distributed Correlation	This rule populates the event counts for distributed correlation to a list.	/All Rules/ArcSight Administration/ESM/Distributed Correlation Monitoring/
Excessive Rule Recursion	This rule detects excessive rule recursion. This rule looks for events coming from the ArcSight Security Manager with the Device Event Category set to /Rule/Warning/Loop. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/
Invalid Resource Deleted	This rule removes an invalid resource from the Invalid Resources active list when that resource is deleted. The rule triggers only if the resource that has been deleted is in the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
License Audit Event Detected	This rule triggers when a license audit event is detected. The rule adds the license type, the current count, and the count limit to the License History session list.	/All Rules/ArcSight Administration/ESM/Licensing/
Logger Sensor Status	This rule identifies Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status with the Logger IP address, the sensor type, the sensor name, and the sensor status. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/

Rule Resources, continued

Resource	Description	URI
Logger Sensor Type Status	This rule identifies Logger Sensor Status correlation events and triggers only if all the sensor statuses for the same sensor type for a Logger are in an OK state. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/
Logger Status	This rule identifies Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger are in an OK state. This rule is disabled by default. Enable the rule if you have Logger in your environment.	/All Rules/ArcSight Administration/Logger/System Health/
Out of Domain Fields	This rule triggers when there is no more free domain field available for a field type.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Domains/
Query Running Time	This rule triggers when a query audit event is detected. The rule adds or updates the corresponding entry in the active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Resource Became Invalid	This rule triggers when a resource becomes invalid. The rule adds the resource ID, name, URI, and type to the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Resource Became Valid	This rule triggers when an invalid resource becomes valid. The rule removes the resource from the Invalid Resources active list.	/All Rules/ArcSight Administration/ESM/System Health/Resources/
Rule Matching Too Many Events	This rule detects rules that match too many events. The rule identifies events that come from the ArcSight Security Manager with the Device Event Category set to /Rule/Error/Deactivate/Unsafe. This rule only requires one such event within five minutes. After this rule is triggered, a notification is sent to the SOC Operators.	/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/
Storage Licensing Audit event Detected	This rule detects connector raw event statistic events and stores them in an active list.	/All Rules/ArcSight Administration/ESM/Licensing/

Rule Resources, continued

Resource	Description	URI
Update Connector Caching Status	This rule detects active list audit events for changes in the related connector caching/dropping active lists. The rule then sets the device custom number and string information to be used by the Connector Cache Status data monitor.	/All Rules/ArcSight Administration/Connectors/System Health/
Update Connector Connection Status	This rule monitors audit events for changes in the connector connection status active lists. The rule then sets the device custom number and the string information used by the Connector Connection Status data monitor.	/All Rules/ArcSight Administration/Connectors/System Health/
Warning - System Resources Exhausted	This rule indicates that a device has detected a system resource issue. The rule triggers whenever a resource is exhausted or a resource check fails. On the first event, a notification is sent to SOC operators. Note: This rule does not produce completely accurate results when running in Turbo Mode Fastest.	/All Rules/ArcSight Administration/ESM/System Health/Resources/

Session Lists

The following table lists all the session lists.

Session List Resources

Resource	Description	URI
ArcSight User Sessions	This session list stores the client username, client address and zone used by an ArcSight user to access the ArcSight Manager to monitor the login times, logout times, or Console timeouts and to determine who had access to the system over specific time periods.	/All Session Lists/ArcSight Administration/ESM/User Access/User Sessions/
Connector - Caches	This session list stores the cache history for all the connectors. A new session is created every time a connector starts caching or dropping events.	/All Session Lists/ArcSight Administration/Connectors/System Health/
Connector Versions	This session list stores the version history for all the connectors. The fields in the session list are: Connector ID, Connector Name, Connector Version, Connector Type, Connector Address, and Connector Zone. The session list is populated by the Connector Upgrade Successful and Connector Version Detected rules.	/All Session Lists/ArcSight Administration/Connectors/Configuration Changes/
Licensing History	This session list stores the licensing history for the various license types. The session list stores the license type, the current count, and the count limit.	/All Session Lists/ArcSight Administration/ESM/Licensing/

Trends

The following table lists all the trends.

Trend Resources

Resource	Description	URI
ASM Database Free Space	This trend stores the free space percentages by hour for the four ASM database table spaces (ARC_EVENT_DATA, ARC_EVENT_INDEX, ARC_SYSTEM_DATA, and ARC_SYSTEM_INDEX).	/All Trends/ArcSight Administration/ESM/System Health/Storage/
ArcSight User Login Trends - Hourly	This trend tracks the counts of how many users logged into ArcSight ESM within the previous hour. The trend checks if the Login tracking rule triggered and then populated a data monitor with currently logged in users.	/All Trends/ArcSight Administration/ESM/User Access/

Trend Resources, continued

Resource	Description	URI
Connector Average EPS - Last 7 days	This trend stores the average EPS for all connectors during the last seven days and writes the data to an active list by leveraging the trend action feature.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Connector Daily Average EPS	This trend stores the daily average EPS for all connectors and writes the data to an active list by leveraging the trend action feature.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Connector Total Events - Hourly	This trend stores the hourly average EPS for all connectors.	/All Trends/ArcSight Administration/Connector/System Health/EPS/
Events Count	This trend stores the total number of non ArcSight events.	/All Trends/ArcSight Administration/ESM/Events Analysis Overview/
Failed Queries	This trend stores failed queries for reports, trends, and query viewers.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Hourly EPS in Persistor	This trend stores hourly EPS in persistor.	/All Trends/ArcSight Administration/ESM/Distributed Correlation Monitoring/
QueryViewer Queries	This trend stores the top longest query viewer queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Report Queries	This trend stores the top longest report queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/
Storage Licensing Data	This trend stores the raw event length reported by the raw event statistic events for each connector.	/All Trends/ArcSight Administration/ESM/Licensing/
Trend Queries	This trend stores the top longest trend queries by day.	/All Trends/ArcSight Administration/ESM/System Health/Resources/Reporting/

Use Cases

The following table lists all the use cases.

Use Case Resources

Resource	Description	URI
ArcSight ESM Device Monitoring	This use case monitors the status of ArcSight ESM devices using the Device Status Monitoring (DSM) functionality that comes with SmartConnectors.	/All Cases/ArcSight Administration/Devices/
Connector Configuration Changes	This use case provides information about configuration changes (such as upgrades) and connector version changes on the system.	/All Cases//All Active Channels/ArcSight Administration/Connectors/
Connector Connection and Cache Status	This use case provides information about the connection status and caching status of connectors in the system. Connectors can be connected directly to ESM or through Loggers.	/All Cases/ArcSight Administration/Connectors/
Connector Overview	This use case covers administration content for monitoring connectors and devices.	/All Cases/ArcSight Administration/
Device Monitoring	This use case provides information about the devices reporting to ESM.	/All Cases/ArcSight Administration/Connectors/
ESM Events	This use case provides statistics about the flow of events through ESM.	/All Cases/ArcSight Administration/ESM/System Health/
ESM Licensing	This use case provides information about ESM licensing compliance.	/All Cases/ArcSight Administration/ESM/
ESM Overview	This use case provides information about administration content for monitoring ESM.	/All Cases/ArcSight Administration/
ESM Reporting Resource Monitoring	This use case provides information about performance statistics for reports, trends, and query viewers.	/All Cases/ArcSight Administration/ESM/System Health/
ESM Resource Configuration Changes	This use case provides information about changes to the ESM resources, such as rules, reports, and so on.	/All Cases/ArcSight Administration/ESM/Configuration Changes/
ESM Resource Monitoring	This use case provides processing statistics for various ESM resources, such as trends, rules, and so on.	/All Cases/ArcSight Administration/ESM/System Health/
ESM User Sessions	This use case provides information about user access to ESM.	/All Cases/ArcSight Administration/ESM/

Use Case Resources, continued

Resource	Description	URI
Logger Events	This use case provides information about statistics for events sent through Loggers to ESM.	/All Cases/ArcSight Administration/Logger/
Logger Overview	This use case provides Logger status and statistics.	/All Cases/ArcSight Administration/
Logger System Health	This use case provides performance statistics for the Loggers connected to ESM.	/All Cases/ArcSight Administration/Logger/

ArcSight CORRE Resources By Type

This section lists all the resources by type.

• Active Lists	80
• Dashboards	81
• Data Monitors	81
• Filters	82
• Focused Reports	83
• Queries	84
• Query Viewers	85
• Reports	85
• Report Templates	86
• Rules	86
• Session Lists	87
• Use Cases	87

Active Lists

The following table lists all the active lists.

CORR-Engine Active List Resources

Resource	Description	URI
Archive Task Failures	This active list stores archive task failure events, which include activation, deactivation, and scheduling.	/All Active Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failures	This active list stores archive archival failure events.	/All Active Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Dashboards

The following table lists all the dashboards.

CORR-Engine Dashboard Resources

Resource	Description	URI
Archive Status	This dashboard shows database archive related information.	/All Dashboards/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Database Performance Statistics	This dashboard shows an overview of database related statistics, such as available space, insert, and retrieval times.	/All Dashboards/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Data Monitors

The following table lists all the data monitors.

CORR-Engine Data Monitor Resources

Resource	Description	URI
Archive Disk Space	This data monitor shows the state of archive disk space used: OK, Warning, and Critical Warning.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/
Database Free Space	This data monitor displays the database free space.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Insert Time - Last 24 Hours	This data monitor displays the moving average for database insert time during the last 24 hours.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Insert Time - Last Hour	This data monitor displays the moving average for database insert time during the last hour.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/

CORR-Engine Data Monitor Resources, continued

Resource	Description	URI
Database Retrieval Time - Last 24 Hours	This data monitor displays the moving average for database retrieval time during the last 24 hours.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Database Retrieval Time - Last Hour	This data monitor displays the moving average for database retrieval time during the last hour.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Database Performance Statistics/
Recent Archive Events	This data monitor shows last ten archive events.	/All Data Monitors/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Archive Status/

Filters

The following table lists all the filters.

CORR-Engine Filter Resources

Resource	Description	URI
Archive Archival Success	This filter selects archive archival success audit events.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Disk Space	This filter selects archive disk space audit events.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Disk space status is Critical	This filter selects archive disk space audit events where custom number 1, which is the Used Space Percentage, is greater than a certain value. 95 is the default number.	/All Filters/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Disk space status is OK	This filter selects archive disk space audit events where custom number 1, which is Used Space Percentage, is less than a certain value. 85 is the default number.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Events	This filter selects all archive audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

CORR-Engine Filter Resources, continued

Resource	Description	URI
Archive Failure Events	This filter selects all archive failure audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
Archive Settings Updated Event	This filter selects archive settings updated audit events.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/
File Path StartsWith All Rules	This filter selects events in which the file path starts with /All Rules.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/Conditional Variable Filters/

Focused Reports

The following table lists all the focused reports.

CORR-Engine Focused Report Resources

Resource	Description	URI
Event Data Free Space - Last 30 Days	This report shows the free space percentages by day for the ARC_EVENT_DATA database table space for the last 30 days. The source report is ASM Database Free Space - by Day.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
System Data Free Space - Last 30 Days	This focused report shows the free space percentages by day for the ARC_SYSTEM_DATA database table space for the last 30 days. The source report is ASM Database Free Space - by Day.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Queries

The following table lists all the queries.

CORR-Engine Query Resources

Resource	Description	URI
Archive Activation Statistics	This query selects archive activation audit events from the Archive Events session list.	/All Queries/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Archival Statistics	This query selects archive archival audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Archival Success	This query selects archive archival information from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Deactivation Statistics	This query selects archive deactivation audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Disk Space Usage	This query selects archive disk space used information from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Non-success events	This query selects non-successful archive audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Scheduling Statistics	This query selects archive scheduling audit events from the Archive Events session list.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Space status	This query selects archive space audit events.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Failure Details	This query selects archive task failure events from the active list: Archive Task Failures.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive status	This query selects archive audit events from the Archive Events session list that have not been terminated, which are the latest event for each archive name.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failure Details	This query selects archive archival failure events from the active list: Critical Archive Failures.	/All Focused Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Query Viewers

The following table lists all the query viewers.

CORR-Engine Query Viewer Resources

Resource	Description	URI
Archive Task Failure Details	This query viewer shows the current archive task failure events, which include activation, deactivation and scheduling.	/All Query Viewers/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failure Details	This query viewer shows the current archive archival failure events.	/All Query Viewers/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Reports

The following table lists all the reports.

CORR-Engine Report Resources

Resource	Description	URI
ASM Database Free Space	This report shows the current free space percentages for the ASM database table spaces. The report shows the percentages for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
ASM Database Free Space - by Day	This report shows the free space percentages by day for one of the ASM database table spaces. The report has one chart and one table, and has a custom parameter that can be used to choose one of the table spaces (ARC_EVENT_DATA or ARC_SYSTEM_DATA, if this is an Oracle installation, ARC_EVENT_INDEX and ARC_SYSTEM_INDEX are also available).	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
ASM Database Free Space - by Hour	This report shows the free space percentages by hour for the ASM database table spaces. The report shows the percentages by hour for the ARC_EVENT_DATA and ARC_SYSTEM_DATA table spaces.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Processing	This report shows the longest to process archives and the time to archive information.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Status Report	This report shows the current status of archive and disk space used.	/All Reports/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Report Templates

The following table lists all the report templates.

CORR-Engine Report Template Resources

Resource	Description	URI
Archive Template	This report template contains two tables. It is designed for the archive status report and includes scripting to make the first column in the tables a color: red, yellow or green, based on the value in another column.	/All Report Templates/ArcSight Administration/System Health/Storage/CORR-Engine/

Rules

The following table lists all the rules.

CORR-Engine Rule Resources

Resource	Description	URI
Archive Events	This rule is triggered by archive audit events and writes to the Archive Events session list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Failures	This rule is triggered by archive task failure events, which include activation, deactivation and scheduling events, and writes to the Archive Task Failures active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Archive Task Success	This rule is triggered by successful archive activation, deactivation, and scheduling audit events where the archive name is in the Archive Task Failures active list. This rule removes the entry from the active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Failures	This rule is triggered by archive archival failure events and writes to the Critical Archive Failures active list.	/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/
Critical Archive Success	This rule is triggered by archive archival success events where the archive name is in the Critical Archival Failures active list. This rule removes the entry from the active list.	/All Rules/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Session Lists

The following table lists all the session lists.

CORR-Engine Session List Resources

Resource	Description	URI
Archive Events	This session list stores archive audit events.	/All Session Lists/ArcSight Administration/ESM/System Health/Storage/CORR-Engine/

Use Cases

The following table lists all the use cases.

CORR-Engine Use Case Resources

Resource	Description	URI
ESM Storage Monitoring (CORR-Engine)	This use case provides information about the health of the CORR Engine (ArcSight Express 3.0 and beyond).	/ArcSight Administration/ESM/System Health/

ArcSight Content Management Resources By Type

This section lists all the resources by type.

- [Active Lists](#) 88
- [Dashboards](#) 88
- [Queries](#) 89
- [Query Viewers](#) 90
- [Reports](#) 91
- [Rules](#) 92
- [Notification Groups](#) 92
- [Use Cases](#) 92

Active Lists

The following table lists all the active lists.

Content Management Active List Resources

Resource	Description	URI
Content Management History	This active list stores data for all the Content Management related events.	/ArcSight Administration/ESM/Content Management/
Content Management History Failure	This active list stores data only for failed Content Management related events.	/ArcSight Administration/ESM/Content Management/

Dashboards

The following table lists all the dashboards.

Content Management Dashboard Resources

Resource	Description	URI
Synchronization Status History	This dashboard shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.	/ArcSight Administration/ESM/Content Management/

Queries

The following table lists all the queries.

Content Management Query Resources

Resource	Description	URI
Top Packages with Synchronization Errors	This query selects information about the content packages with the most issues related to either package update delivery or installation after the package has been delivered.	/ArcSight Administration/ESM/Content Management/
Top Subscribers with Errors	This query selects information about the subscribers experiencing the most issues with managed package delivery or installation.	/ArcSight Administration/ESM/Content Management/
Top Synchronization Errors	This query selects information about the most common issues with the delivery or installation of managed packages.	/ArcSight Administration/ESM/Content Management/
Content Management Failure	This query selects information about Content Management failure events that have occurred recently.	/ArcSight Administration/ESM/Content Management/

Query Viewers

The following table lists all the query viewers.

Content Management Query Viewer Resources

Resource	Description	URI
Top Packages with Synchronization Errors	This query viewer displays information about the content packages with the most issues related to either package update delivery or to installation after the package has been delivered.	/ArcSight Administration/ESM/Content Management/
Top Subscribers with Errors	This query viewer displays information about the subscribers experiencing the most issues with managed package delivery or installation.	/ArcSight Administration/ESM/Content Management/
Top Synchronization Errors	This query viewer displays information about the most common issues with delivery or installation of managed packages.	/ArcSight Administration/ESM/Content Management/
Content Management Failure	This query viewer displays information about Content Management Failure events that have occurred recently.	/ArcSight Administration/ESM/Content Management/

Reports

The following table lists all the reports.

Content Management Report Resources

Resource	Description	URI
Synchronization Status History	This report shows information about the history of content packages synchronized across peered Arcsight Managers or subscribers.	/ArcSight Administration/ESM/Content Management/
Top Packages with Synchronization Errors	This report shows information about the content packages with the most update delivery issues or installation issues after the package has been delivered.	/ArcSight Administration/ESM/Content Management/
Top Subscribers with Errors	This report shows information about the subscribers experiencing the most issues with managed package delivery or installation.	/ArcSight Administration/ESM/Content Management/
Top Synchronization Errors	This report shows information about the most common issues experienced by subscribers with managed package delivery or installation.	/ArcSight Administration/ESM/Content Management/

Rules

The following table lists all the rules.

Content Management Rule Resources

Resource	Description	URI
Content Management Data	This rule maintains the Content Management History active list.	/ArcSight Administration/ESM/Content Management/
Content Management Data Failure	This rule sends a notification to the Content Management notification group each time a failure event occurs. Also, this rule maintains the Content Management History Failure active list.	/ArcSight Administration/ESM/Content Management/

Notification Groups

The following table lists all the notification groups.

Content Management Notification Group Resources

Resource	Description	URI
Content Management	This notification group receives a notification when a Content Management event fails.	/ArcSight Administration/ESM/Content Management/

Use Cases

The following table lists all the use cases.

Content Management Use Case Resources

Resource	Description	URI
Content Management	This use case contains resources that track content that is managed across multiple ESM systems with the Content Management feature.	/ArcSight Administration/ESM/Content Management/

Transformation Hub Monitoring Resources by Type

This section lists all the resources by type.

- [Active Channels](#)93
- [Active Lists](#) 93
- [Dashboards](#)94
- [Data Monitors](#)94
- [Field Sets](#)94
- [Filters](#)95
- [Queries](#)95
- [Query Viewers](#)95
- [Rules](#)96

Active Channels

The following table lists all the active channels.

Transformation Hub Monitoring Active Channel Resources

Resource	Description	URI
Transformation Hub Audit Events	This active channel shows Transformation Hub audit events.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Active Lists

The following table lists all the active lists.

Transformation Hub Monitoring Active List Resources

Resource	Description	URI
Event Counts from Transformation Hub	This list holds information on EB Address and Port, Topic Name, Hour of Day, and total count of events as detected by the Transformation Hub rule.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Dashboards

The following table lists all the dashboards.

Transformation Hub Monitoring Dashboard Resources

Resource	Description	URI
Transformation Hub Monitoring	This dashboard displays Transformation Hub monitoring.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Data Monitors

The following table lists all the data monitors.

Transformation Hub Monitoring Data Monitor Resources

Resource	Description	URI
Transformation Hub Status	This data monitor shows status of Transformation Hub.	/ArcSight Administration/ESM/Transformation Hub Monitoring/
Message Count Remaining in Transformation Hub	This data monitor shows status of message count remaining in Transformation Hub.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Field Sets

The following table lists all the field sets.

Transformation Hub Monitoring Field Set Resources

Resource	Description	URI
Transformation Hub	This field set is for Transformation Hub monitoring.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Filters

The following table lists all the filters.

Transformation Hub Monitoring Filter Resources

Resource	Description	URI
Transformation Hub Audit Events	This filter selects all Transformation Hub audit events.	/ArcSight Administration/ESM/Transformation Hub Monitoring/
Message Count Remaining in Transformation Hub	This filter selects audit events for messages remaining in Transformation Hub.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Queries

The following table lists all the queries.

Transformation Hub Monitoring Query Resources

Resource	Description	URI
EPS Forwarded from Transformation Hub	This query retrieves EPS count for events sent from Transformation Hub.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Query Viewers

The following table lists all the query viewers.

Transformation Hub Monitoring Query Viewer Resources

Resource	Description	URI
Hourly EPS Forwarded from Transformation Hub	This query viewer displays hourly EPS count forwarded from Transformation Hub.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

Rules

The following table lists all the rules.

Transformation Hub Monitoring Rule Resources

Resource	Description	URI
Detect Events for Transformation Hub	This rule triggers when eventbroker:103 (Event Count forwarded to ESM) event occurs. This rule populates the Event Counts from Transformation Hub active list every hour.	/ArcSight Administration/ESM/Transformation Hub Monitoring/

ESM Active Passive High Availability (APHA) Monitoring Resources By Type

This section lists all the resources by type.

- [Active Channels](#)97
- [Active Lists](#) 97
- [Dashboards](#)98
- [Data Monitors](#)98
- [Field Sets](#)98
- [Filters](#)100
- [Queries](#)100
- [Query Viewers](#)101
- [Reports](#)101
- [Rules](#)102
- [Session Lists](#)102
- [Use Cases](#)102

Active Channels

The following table lists all the active channels.

ESM APHA Monitoring Active Channel Resources

Resource	Description	URI
APHA Monitoring	This active channel shows APHA status events.	/ArcSight Administration/ESM/APHA Monitoring/

Active Lists

The following table lists all the active lists.

ESM APHA Active List Resources

Resource	Description	URI
Current Primary System	This active list is populated by the ESM System Started rule. The active list is used by a query to retrieve the IP address and hostname of the current Primary System. This information is then displayed in the ESM APHA Status dashboard.	/ArcSight Administration/ESM/APHA Monitoring/

Dashboards

The following table lists all the dashboards.

ESM APHA Dashboard Resources

Resource	Description	URI
ESM APHA Status	This dashboard shows an overview of the ESM APHA state. The top panel shows the current APHA state. The second panel shows the IP address and hostname of the current Primary System. The third panel shows ESM system changes, such as a Manager restart or APHA failover during the last 24 hours. The bottom panel shows the last ten APHA status changes.	/ArcSight Administration/ESM/APHA Monitoring/

Data Monitors

The following table lists all the data monitors.

ESM APHA Data Monitor Resources

Resource	Description	URI
ESM APHA Status	This data monitor shows the current ESM APHA status.	/ArcSight Administration/ESM/APHA Monitoring/
Last 10 APHA Status Changes	This data monitor shows the last ten APHA status changes.	/ArcSight Administration/ESM/APHA Monitoring/

Field Sets

The following table lists all the field sets.

ESM APHA Field Set Resources

Resource	Description	URI
APHA Management	This field set contains fields used to examine APHA status events.	/ArcSight Administration/ESM/APHA Monitoring/

Filters

The following table lists all the filters.

ESM APHA Filter Resources

Resource	Description	URI
ESM APHA Status	This filter detects events generated by the APHA module.	/ArcSight Administration/ESM/APHA Monitoring/

Queries

The following table lists all the queries.

ESM APHA Query Resources

Resource	Description	URI
Current Primary System	This query retrieves details for the current Primary System from the Current Primary System active list. The details are displayed in the ESM APHA Status dashboard.	/ArcSight Administration/ESM/APHA Monitoring/
Current Primary System Details	This query retrieves details for the Primary System from the Current Primary System Status Change session list. It is used for the query viewer, which is in turn used in the dashboard drilldown.	/ArcSight Administration/ESM/APHA Monitoring/
ESM APHA Status - last 7 days	This query retrieves details of the APHA module status changes within the last seven days. It is used in the ESM APHA Status Updates - last 7 days report.	/ArcSight Administration/ESM/APHA Monitoring/
System Status Changes	This query retrieves Primary System status change details from the Current Primary System Status Change session list. It is used for the query viewer, which is in turn used in the dashboard drilldown.	/ArcSight Administration/ESM/APHA Monitoring/
System Status Changes - Last 24 hours	This query retrieves details for the ESM System status changes (restarts or APHA failovers) from the Current Primary System Status Change session list. It is used by the query viewer to populate the data in the dashboard.	ArcSight Administration/ESM/APHA Monitoring/

Query Viewers

The following table lists all the query viewers.

ESM APHA Query Viewer Resources

Resource	Description	URI
Current Primary System	This query viewer displays details for the current Primary System.	/ArcSight Administration/ESM/APHA Monitoring/
Current Primary System Details	This query viewer displays details for the Primary System. It is used for the dashboard drilldown.	/ArcSight Administration/ESM/APHA Monitoring/
System Status Changes	This query viewer displays details for the ESM System status changes (restarts or APHA failovers). It is used for the dashboard drilldown.	/ArcSight Administration/ESM/APHA Monitoring/
System Status Changes - Last 24 hours	This query viewer displays details about the ESM System status changes (restarts or APHA failovers). The information is displayed in the dashboard.	/ArcSight Administration/ESM/APHA Monitoring/

Reports

The following table lists all the reports.

ESM APHA Report Resources

Resource	Description	URI
ESM APHA Status Updates - last 7 days	This report shows all APHA status updates within the last seven days.	/ArcSight Administration/ESM/APHA Monitoring/

Rules

The following table lists all the rules.

ESM APHA Rule Resources

Resource	Description	URI
Alert - APHA Status Change	This rule triggers when an APHA status change event is generated. After the rule triggers, a notification is sent to the SOC Operators team.	/ArcSight Administration/ESM/APHA Monitoring/
ESM System Started	This rule triggers when a Primary System starts up; for example, the ESM manager restarts or there is an APHA failover. After the rule triggers, the entry is created or updated in the Current Primary System active list and in the Current Primary System Status Change session list.	/ArcSight Administration/ESM/APHA Monitoring/

Session Lists

The following table lists all the session lists.

ESM APHA Session List Resources

Resource	Description	URI
Current Primary System Status Change	This session list is populated by the ESM System Started rule. It stores a history of the Primary System restarts and failovers. A new session is created every time a system restarts or the APHA failover occurs. This session list is used by the query to retrieve the system status changes and populates the APHA Monitoring dashboard and the ESM APHA Status Updates - last 7 days report.	/ArcSight Administration/ESM/APHA Monitoring/

Use Cases

The following table lists all the use cases.

ESM APHA Use Case Resources

Resource	Description	URI
APHA Monitoring	This use case monitors the status of the ESM APHA Module (APHA module).	/ArcSight Administration/ESM/APHA Monitoring/

ArcSight Foundation Resources

This chapter lists all the resources by type in the ArcSight Foundation packages.

- [ArcSight ClusterView Resources By Type](#) 105
 - [Data Monitors](#) 105
 - [Fields](#) 106
- [ArcSight SOCVIEW Resources By Type](#) 107
 - [Data Monitors](#) 107
 - [Filters](#) 108
 - [Query Viewers](#) 108
 - [Queries](#) 108
- [Security Threat Monitoring Resources By Type](#) 109
 - [Fields](#) 110
 - [Field Sets](#) 111
 - [Active Channels](#) 112
 - [Active Lists](#) 113
 - [Dashboards](#) 114
 - [Data Monitors](#) 115
 - [Filters](#) 117
 - [Packages](#) 120
 - [Queries](#) 121
 - [Query Viewers](#) 122
 - [Rules](#) 123
 - [Use Cases](#) 127
- [Security Monitoring - Base Resources By Type](#) 129
 - [Active Channels](#) 130
 - [Active Lists](#) 131
 - [Data Monitors](#) 132
 - [Dashboards](#) 133
 - [Fields](#) 134
 - [Field Sets](#) 136
 - [Filters](#) 137
 - [Integration Commands](#) 138
 - [Integration Configurations](#) 139

• Packages	140
• Queries	141
• Query Viewers	142
• Rules	143
• Reports	144
• Use Cases	145
• Security Monitoring - Base - Active Lists Resources By Type	146
• Active Lists	147
• Packages	148
• Threat Intelligence Platform Resources By Type	149
• Filters	150
• Fields	151
• Active Lists	158
• Integration Commands	160
• Integration Configurations	161
• Packages	162
• Rules	163
• Dashboards	166
• Queries	167
• Query Viewers	168
• Use Cases	169
• Common Resources By Type	170
• Conditional Variable Filters	170
• Network Filters	179
• Variables Library Fields	180

ArcSight ClusterView Resources By Type

This section lists all ClusterView Resources by type.

- [Data Monitors](#)105
- [Fields](#)106

Data Monitors

The following table lists all the data monitors.

ArcSight ClusterView Data Monitor Resources

Resource	Description	URI
Aggregator Audit Events	Data Monitor to display Aggregator Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Correlator Audit Events	Data Monitor to display Correlator Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/
Distributed Correlation Audit Events	Data Monitor to display Distributed Mode Audit Events	/All Data Monitors/ArcSight Foundation/ArcSight ClusterView/

Fields

The following table lists all the fields.

ArcSight ClusterView Field Resources

Resource	Description	URI
Service Message	This variable returns service message for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/
Service Name And ID	This variable returns name and ID for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/
Message Type	This variable returns service message type for distributed correlation audit events.	/All Fields/ArcSight Foundation/ArcSight ClusterView/

ArcSight SOCView Resources By Type

This section lists all SOCView Resources by type.

- [Data Monitors](#)107
- [Filters](#)108
- [Query Viewers](#)108
- [Queries](#)108

Data Monitors

The following table lists all the data monitors.

ArcSight SocView Data Monitor Resources

Resource	Description	URI
Live Activity	This data monitor shows non-Arcsight internal live events.	/All Filters/ArcSight Foundation/ArcSight SocView/
Malicious Activity	This data monitor shows malicious activity.	/All Filters/ArcSight Foundation/ArcSight SocView/
Rule Counts	This data monitor shows rule correlation event count.	/All Filters/ArcSight Foundation/ArcSight SocView/
Rules Activity	This data monitor shows rule correlation events.	/All Filters/ArcSight Foundation/ArcSight SocView/
Top Attack Types	This data monitor shows top attack types.	/All Filters/ArcSight Foundation/ArcSight SocView/
Top Destination Address	This data monitor shows top destination addresses.	/All Filters/ArcSight Foundation/ArcSight SocView/
Top Source Address	This data monitor shows top source addresses.	/All Filters/ArcSight Foundation/ArcSight SocView/
Top Source Geo	This data monitor shows top source geo.	/All Filters/ArcSight Foundation/ArcSight SocView/

Filters

The following table lists all the filters.

ArcSight SocView Filter Resources

Resource	Description	URI
Live Activity	This filter selects non-arcSight internal events.	/All Filters/ArcSight Foundation/ArcSight SocView/
Malicious Activity	This filter selects malicious activity detected by antivirus.	/All Filters/ArcSight Foundation/ArcSight SocView/
Rule Activity	This filter selects rule correlation events.	/All Filters/ArcSight Foundation/ArcSight SocView/

Query Viewers

The following table lists the query viewers.

ArcSight SocView Query Viewer Resources

Resource	Description	URI
Asset Counts	This query viewer shows number of assets.	/All Query Viewers/ArcSight Foundation/ArcSight SocView/

Queries

The following table lists the queries.

ArcSight SocView Query Resources

Resource	Description	URI
Number of Assets	This query selects number of assets.	/All Queries/ArcSight Foundation/ArcSight SocView/

Security Threat Monitoring Resources By Type

This section lists all Security Threat Monitoring Resources by type.

• Fields	110
• Field Sets	111
• Active Channels	112
• Active Lists	113
• Dashboards	114
• Data Monitors	115
• Filters	117
• Packages	120
• Queries	121
• Query Viewers	122
• Rules	123
• Use Cases	127

Fields

The following table lists all the fields.

Security Threat Monitoring Field Resources

Resource	Description	URI
getExploitingCategory	This variable returns category for exploit from a list.	/All Fields/ArcSight Foundation/Security Threat Monitoring/
getInterZoneCommunications	This variable returns service information from the interzone communications to restricted services list.	/All Fields/ArcSight Foundation/Security Threat Monitoring/

Field Sets

The following table lists all the field sets.

Security Threat Monitoring Field Set Resources

Resource	Description	URI
Attacks and Suspicious Activity	This field set contains essential fields required to investigate attacks and suspicious activity through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Main Channel	This field set contains essential fields required to investigate Entity Monitoring rules and correlation events through active channels.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Vulnerable Asset	This field set displays event field information about asset vulnerabilities.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
DNS DGA	This field set contains event fields used to investigate DNS DGA events.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful Logins	This field set contains essential fields required to investigate brute force attacks through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Members Added and Removed from Groups	This field set contains essential fields required to investigate members added and removed from groups through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Malware Events	This field set contains event fields used to investigate malware events.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/
Brute Force Login	This field set contains essential fields required to investigate brute force attack through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/

Active Channels

The following table lists all the active channels.

Security Threat Monitoring Active Channel Resources

Resource	Description	URI
Entity Monitoring Main Channel	This active channel shows all the entity monitoring category correlation events in the last hour.	/All Active Channels/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful Logins	This active channel shows unsuccessful logins in the last hour.	/All Active Channels/ArcSight Foundation/Security Threat Monitoring/

Active Lists

The following table lists all the active lists.

Security Threat Monitoring Active List Resources

Resource	Description	URI
Brute Force Attempts	This active list stores information about suspected brute force attempt events. The Brute Force IDS Detected Attempts and Brute Force OS and Application Attempts rules update this active list with attacker system, user account, and target system information.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/
Malware Target Based Suppression	This suppression list is based on target address and generator name.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/
User Account Created	This active list stores the information about the user accounts created within the organization. This active list is updated automatically by a rule and it is used by another rule. By default, the list expires in 24 hours.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/
User Accounts Added to Group	This active list stores the information about the user accounts added to groups within the organization. This active list is updated automatically by a rule and it is used by another rule. By default, the list expires in 24 hours.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/
Host Name Based Suppression	This suppression list is based on device host name and generator.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/

Dashboards

The following table lists all the dashboards.

Security Threat Monitoring Dashboard Resources

Resource	Description	URI
Unsuccessful Logins from different Countries	This dashboard provides overview of unsuccessful logins from different countries	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
DNS DGA Monitoring	This dashboard displays DNS DGA statistics.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
Malware Activity	This dashboard displays malware statistics.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
Members Added and Removed from Privileged Groups	This dashboard provides information about members that were added and removed from the privileged group.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
Attacks and Suspicious Activity Overview	This dashboard provides overview of attacks and suspicious activities based on ArcSight categorization events.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
Brute Force Attack Detection Dashboard	This dashboard presents overview of suspected Brute Force Attacks.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/
Vulnerability Overview	This dashboard displays data related to vulnerable assets.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/

Data Monitors

The following table lists all the data monitors.

Security Threat Monitoring Data Monitor Resources

Resource	Description	URI
Top 10 Attackers	This data monitor displays the top 10 attacker IP addresses.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top Malicious Domains Accessed	This data monitor displays top DGA domains being accessed by hosts.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Security Indicator - Systems Experiencing High Volume of Failed Logins	This data monitor displays top 10 counts of failed authentication events, grouped by target IP address.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Successful Brute Force Login	This data monitor displays the last 5 successful brute force logins.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Brute Force Attack Attempts	This data monitor displays the last 5 brute force attacks attempts.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Security Indicator - Failed Login Count by User Account	This data monitor displays top 10 counts of failed authentication events, grouped by user account.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top 10 Attacker Countries	This data monitor shows the top 10 attacker countries.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top Addresses Communicating With Malicious Domains	This data monitor displays top addresses that are trying to communicate with malicious domains on the network.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top Vulnerable Asset under Attack	This data monitor displays top assets having vulnerability under attack.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Data Monitor Resources, continued

Resource	Description	URI
Security Indicator - Most Active Failed Login Source Systems	This data monitor displays top 10 counts of failed authentication events, grouped by attacker IP address.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Members Added and Removed from Privileged Group within 24 Hours	This data monitor displays the last 5 members that were added and removed from the Privileged Group within 24 Hours.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Attacks and Suspicious Activity per 10 Minutes	This data monitor shows a moving average of attacks. It displays data for the last 10 minutes and generates a correlation event if the moving average increases by 300%.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top Malware Names Infections	This data monitor displays top malware names infecting devices.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
All Unsuccessful Logins from different Countries - GeoView	This data monitor shows all the unsuccessful logins from different countries on a map.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Latest Malware Infections on Critical Assets	This data monitor displays latest malware infection on High and Very Critical assets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top Addresses With Malware Infections	This data monitor displays top addresses having malware infections.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Top 10 Targets	This data monitor displays the top 10 attacks and suspicious activity targets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful Login Count by Country	This data monitor displays top 10 counts of failed authentication events, grouped by source country.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Last 10 Attacks and Suspicious Activity Events	This data monitor displays the last 10 attack and suspicious activity events.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/
Latest Attack on Vulnerable Asset	This data monitor displays the latest attacks against vulnerable assets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/

Filters

The following table lists all the filters.

Security Threat Monitoring Filter Resources

Resource	Description	URI
A Member was Added and Removed from Privileged Group within 24 Hours	This filter detects when a user was added and removed from a privileged group using windows events in the last 24 hours.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Windows File Inclusions	This filter captures the most common form of file inclusions to a windows server during a code injection attack	/All Filters/ArcSight Foundation/Security Threat Monitoring/
SQL Injection Attempts from Other Devices	This filter identifies the SQL Injection attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Malware Detected - Critical Assets	This filter detects correlation events generated from Malware Detected Rule for High and Very High critical assets.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful Logins	This filter identifies failed logins by both administrative and non-administrative users.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
A Member was Added into a Group	This filter detects when a user was added into a group using windows events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Login Attempts	This filter selects all attempts to log into systems. It excludes machine logins into Microsoft Windows systems.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Account Lockouts	This filter identifies account lockouts. It recognizes lockouts on Microsoft Windows and Unix systems by default.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Windows Events with a Non-Machine User	This filter identifies Microsoft Windows events that have a non-machine/system user either in the attacker or the target fields.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Cross Site Scripting from Other Devices	This filter identifies Cross Site Scripting attacks from other Device Vendors.	/All Filters/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Filter Resources, continued

Resource	Description	URI
Successful Brute Force Login	This filter searches for correlation events generated by the rule: Successful Brute Force Login .	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful Logins with Geo Information	This filter selects failed login events from different countries with populated Geo fields for both the attacker and target addresses.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
DNS DGA	This filter captures events that the Microsoft DNS DGA Connector reports as randomly generated domains used by attackers to evade detection.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
All Firewall Deny Traffic	This filter identifies events that indicate denied traffic from firewalls.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Brute Force Attack Attempts	This filter searches for correlation events generated by the rules: Brute Force OS and Application Attempts and Brute Force IDS Detected Attempts .	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Malware Detected	This filter detects correlation events generated from the Malware Detected Rule. Such events are alerts about host malware infection.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Attack Vulnerable Asset	This filter detects assets having vulnerabilities.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Account Deletion	This filter identifies account deletion events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Service Stopped	This filter identifies service stop events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Code Injections from Other Devices	This filter identifies the code injection attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
All IDS Events	This filter captures all IDS events based on Categorization.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Source and Destination Address not Null	This filter identifies events in which the source and destination addresses are not null.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Service Failed	This filter identifies service failed events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Filter Resources, continued

Resource	Description	URI
A Member was Removed from a Group	This filter detects when a user was removed from a group using Windows events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Linux File Inclusions	This filter captures the most common form of file inclusions to a Linux server during a code injection attack.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
All Firewall Accept Traffic	This filter identifies events that indicate accepted traffic from firewalls.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Account Creation	This filter identifies account creation events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Web Server Activity Events	This filter captures all web server activity related events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/
Attacks and Suspicious Activity	This filter identifies events that indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Foundation/Security Threat Monitoring/

Packages

The following table lists all the packages.

Security Threat Monitoring Package Resources

Resource	Description	URI
Security Threat Monitoring	This package contains default security threat monitoring content.	/All Packages/ArcSight Foundation/Security Threat Monitoring/

Queries

The following table lists all the queries.

Security Threat Monitoring Query Resources

Resource	Description	URI
Top Addresses With Malware Infections	This query pulls top hosts infected from the Malware Target Based Suppression active list.	/All Queries/ArcSight Foundation/Security Threat Monitoring/
Top Malware Name Infections	This query pulls top malware names infecting devices.	/All Queries/ArcSight Foundation/Security Threat Monitoring/
Asset Vulnerability	This query searches for assets associated with vulnerabilities.	/All Queries/ArcSight Foundation/Security Threat Monitoring/
Last 10 Members Added into a Privileged Group	This query displays the last 10 accounts that were added to a privileged group and not removed within 24 hours.	/All Queries/ArcSight Foundation/Security Threat Monitoring/
All Malware Infections	This query pulls all malware alerts from the Malware Target Based Suppression active list.	/All Queries/ArcSight Foundation/Security Threat Monitoring/

Query Viewers

The following table lists all the query viewers.

Security Threat Monitoring Query Viewer Resources

Resource	Description	URI
Top Addresses With Malware Infections	This query viewer displays top addresses with malware infections.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/
Top Malware Name Infections	This query viewer displays top malware names infecting devices.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/
Asset Vulnerability	This query viewer displays assets with vulnerabilities.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/
Members Added into a Privileged Group	This query viewer displays the last 10 accounts that were added to a privileged group and not removed within 24 hours.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/
All Malware Infections	This query viewer displays all malware alerts.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/

Rules

The following table lists all the rules.

Security Threat Monitoring Rule Resources

Resource	Description	URI
A Member was Added and Removed from Privileged Group within 24 Hours	This rule detects when a user was added and removed from a privileged group using windows events in the last 24 hours.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
User Account Created and Deleted within 24 Hours	This rule identifies an anomalous behavior of user account creation and then deletion within 24 hours (Default TTL: 24 Hours). The rule triggers a correlation event that is sent to a Triage main channel. This rule uses an active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
A Member was Added into a Privileged Group	This rule detects when a user was added into a privileged group using Windows events.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Egress DNS Communications Passed by Firewall	This rule detects Egress DNS communications passed by the firewall.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
User Account Created	This rule fires when a user account is created.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Successful Brute Force Login	This rule searches for a successful authentication event after suspected brute force attempt. The rule triggers when the user account, attacker system, and target system information of successful authentication event matches an entry in the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Multiple Failed Login to Different Accounts from Single Source	This rule fires when multiple failed logins to different accounts from the same source is detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Cleartext Protocol Crossing a Perimeter	This rule detects the Cleartext protocols that cross a perimeter.	/All Rules/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Rule Resources, continued

Resource	Description	URI
Detected Cross Site Scripting	This rule triggers when it detects cross site scripting attacks to the application server through the request URLs, and other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Consecutive Unsuccessful Logins to Same Account from different IPs	This rule fires when a set of 3 consecutive unsuccessful logins to the same account from 3 different IP addresses are detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
High Severity IDS Event	This rule detects all the high severity exploit attacks simulated through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Consecutive Unsuccessful Logins to Same Account from different Countries	This rule fires when a set of 3 consecutive unsuccessful logins to the same account from 3 different countries are detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Attack To Vulnerable Asset	This rule fires when an exploitation attempt on a vulnerable asset is detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Multiple Unique IDS Events to Same Destination	This rule detects multiple unique IDS events gathering information from IDS. This rule gets triggered only when there are 4 unique IDS events in a span of 30 minutes to the same destination.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Pass The Hash	This rule detects Pass The Hash attack attempts on Windows machines. On each detection, the rule adds a target address in the suppression list to avoid sending multiple alerts to the same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Multiple Services Down on Same Host	This rule fires when multiple services go down on the same host in a 30 minute lapse. On each detection, the rule adds a target address in the suppression list to avoid sending multiple alerts on the same address in a short period of time. This rule is disabled by default due to possible performance impact.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Authentication Attempted to Disabled Account	This rule detects authentication attempted to disabled account.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Privileged Account Locked Out	This rule detects account lockouts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Rule Resources, continued

Resource	Description	URI
High Volume of Denies to Same Destination	This rule detects a high volume of denies to the same destination.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Malware Detected	This rule fires when malware activities on the devices are detected. On each detection, the rule adds a target address in the suppression list to avoid sending multiple alerts on same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Detected Code Injection	This rule triggers when it detects code injections attacks to the application server via the request URLs and other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Exploit Attempt Detected by IDS	This rule detects exploit attacks through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Detected SQL Injection	This rule triggers when it detects SQL Injection attacks to the application server through the request URLs and other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Privilege Escalation Attempt Detected	This rule detects privileged exploit attacks through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Brute Force IDS Detected Attempts	This rule searches for brute force attack attempts detected by IDS. The rule triggers when ArcSight ESM receives a brute force attack attempt event from IDS. On occurrence of the first event, the user account, attacker system, and target system information is added to the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Audit Cleared Log	This rule fires when an audit log cleared event is detected. On each detection, the rule adds a target address in the suppression list to avoid sending multiple alerts on the same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Multiple Access Attempts To Malicious Domains From Same Source Address	This rule detects multiple access attempts on malicious domains from the same source address.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Consecutive Unsuccessful Logins to Administrative Account	This rule fires when a set of 5 consecutive unsuccessful logins to an administrative account within 1 minute is detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Rule Resources, continued

Resource	Description	URI
Egress Restricted Services Communications Passed by Firewall	This rule detects egress communications to restricted services passed by the firewall.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Egress Communications to Suspicious Country	This rule detects egress communications to a suspicious country.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
Brute Force OS and Application Attempts	This rule searches for brute force attacks on the OS and applications. The rule triggers when a failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold. On first threshold, information about user account, attacker system, and target system is added to the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/
DoS Activity Detected by IDS	This rule detects Network Denial of Service attacks by gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/

Use Cases

The following table lists all the use cases.

Security Threat Monitoring Use Case Resources

Resource	Description	URI
Network Monitoring	This use case contains resources for network monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Malware Monitoring	This use case contains resources that are included in malware monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Security Threat Monitoring	This is a master use case and contains multiple child use cases.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Account Activity	This use case includes different resources to monitor the below account activities: <ul style="list-style-type: none">• Authentication Attempts to Disabled Account.• Privileged Account Locked Out.• Members added and removed from privileged groups within 24 hours.• User Accounts created and deleted within 24 hours.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Unsuccessful User Logins	This use case includes different resources to monitor the below unsuccessful login activities: <ul style="list-style-type: none">• Consecutive Unsuccessful Logins to Administrative Account.• Consecutive Unsuccessful Logins to Same Account from different Countries.• Consecutive Unsuccessful Logins to Same Account from different IPs.• Multiple Failed Login to Different Accounts from Single Source.• General Unsuccessful Logins.• Failed Login count by user accounts, source and destination systems.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Brute Force Attacks	This use case tracks brute force login attempts and generates alerts for successful brute force attacks.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Vulnerability Monitoring	This use case contains resources that are included in vulnerability monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/

Security Threat Monitoring Use Case Resources, continued

Resource	Description	URI
Host Monitoring	This use case contains resources that are included in host monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Perimeter Monitoring	This use case focuses on events regarding boundary transitions and connections between entities.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Application Monitoring	This use case contains resources for application monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Attacks and Suspicious Activity Overview	This use case includes different resources to monitor attacks and suspicious activity reported by ArcSight Connectors based on ArcSight categorization.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/

Security Monitoring - Base Resources By Type

This section lists all Security Monitoring - Base Resources by type.

• Active Channels	130
• Active Lists	131
• Data Monitors	132
• Dashboards	133
• Fields	134
• Field Sets	136
• Filters	137
• Integration Commands	138
• Integration Configurations	139
• Packages	140
• Queries	141
• Query Viewers	142
• Rules	143
• Reports	144
• Use Cases	145

Active Channels

The following table lists all the active channels.

Security Monitoring - Base Active Channel Resources

Resource	Description	URI
MITRE ATT&CK	This channel shows all correlation rules with MITRE ATT&CK information.	/All Active Channels/ArcSight Foundation/MITRE ATT&CK/

Active Lists

The following table lists all the active lists.

Security Monitoring - Base Active List Resources

Resource	Description	URI
Attacker and Target Based Suppression	This suppression list is based on attacker address, target address, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Rules Triggered with MITRE ID	This list stores MITRE ATT&CK information from correlation rules.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/
Username Based Suppression	This suppression list is based on target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Target Based Suppression	This suppression list is based on target address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Target and Username Based Suppression	This suppression list is based on target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Attacker and Target and Username Based Suppression	This suppression list is based on attacker address, target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Attacker Based Suppression	This suppression list is based on attacker address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/

Data Monitors

The following table lists all the data monitors.

Security Threat Monitoring Data Monitor Resources

Resource	Description	URI
Top Fired MITRE ATT&CK Rules	This data monitor displays the top 5 fired rules with MITRE ATT&CK information.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Top Target IPs	This data monitor displays the top 5 target IP addresses with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
MITRE Attackers and Targets Relations	This data monitor shows relationship between attacker and target machines using MITRE IDs.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Last MITRE ATT&CK Events	This data monitor displays the last 5 MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Top Target Users	This data monitor displays the top 5 users with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/

Dashboards

The following table lists all the dashboards.

Security Monitoring - Base Dashboard Resources

Resource	Description	URI
MITRE ATT&CK Targets Overview	This dashboard provides overview of MITRE ATT&CK events with targets information.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/
MITRE ATT&CK Overview	This dashboard displays MITRE ATT&CK overview.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/

Fields

The following table lists all the fields.

Security Threat Monitoring Field Resources

Resource	Description	URI
mitreName	This variable converts mitre name from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_srcDnsDomain	This variable returns source dns domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_tgtHostName	This variable returns target hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_dstDnsDomain	This variable returns destination dns domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_srcHostName	This variable returns source hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_atkHostName	This variable returns attacker host name in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_dstUserName	This variable returns destination username in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_tgtDnsDomain	This variable returns target dns domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_srcUserName	This variable returns source username in uppercase.	/All Fields/ArcSight Foundation/Common/
getMitre	This variable returns MITRE ATT&CK information.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_tgtUserName	This variable returns target username in uppercase.	/All Fields/ArcSight Foundation/Common/

Security Threat Monitoring Field Resources, continued

Resource	Description	URI
dc_atkUserName	This variable returns attacker user name in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_atkDnsDomain	This variable returns attacker dns domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_dstHostName	This variable returns destination hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
taticName	This variable converts mitre tactic from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
mitreID	This variable converts mitre ID from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_nullString	This variable returns null string.	/All Fields/ArcSight Foundation/Common/

Field Sets

The following table lists all the field sets.

Security Monitoring Base Field Set Resources

Resource	Description	URI
MITRE ATT&CK	This field set selects fields related MITRE ATT&CK.	/All Field Sets/ArcSight Foundation/MITRE ATT&CK/

Filters

The following table lists all the filters.

Security Monitoring - Base Filter Resources

Resource	Description	URI
MITRE ATT&CK with Attacker and Target	This filter selects events with MITRE ATT&CK information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/
MITRE ATT&CK	This filter selects events with MITRE ATT&CK information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/

Integration Commands

The following table lists all the integration commands.

Security Monitoring - Base Integration Command Resources

Resource	Description	URI
MITRE ATT&CK Lookup	This integration command is used to lookup for MITRE ATT&CK technique details.	/All Integration Commands/ArcSight Foundation/MITRE ATT&CK/

Integration Configurations

The following table lists all the integration configurations.

Security Monitoring - Base Integration Configuration Resources

Resource	Description	URI
MITRE ATT&CK Lookup	This integration configuration is used to configure the MITRE ATT&CK lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/MITRE ATT&CK/

Packages

The following table lists all the packages.

Security Monitoring - Base Package Resources

Resource	Description	URI
Security Monitoring - Base	This package contains shared resources required by Security Threat Monitoring and Threat intelligence Platform.	/All Packages/ArcSight Foundation/Security Monitoring - Base/

Queries

The following table lists all the queries.

Security Monitoring Base Query Resources

Resource	Description	URI
MITRE Details Summary	This query selects mitre details summary.	/All Queries/ArcSight Foundation/MITRE ATT&CK/
MITRE by Tactic	This query selects mitre by tactic.	/All Queries/ArcSight Foundation/MITRE ATT&CK/
MITRE by ID	This query selects mitre id.	/All Queries/ArcSight Foundation/MITRE ATT&CK/

Query Viewers

The following table lists all the query viewers.

Security Monitoring - Base Query Viewer Resources

Resource	Description	URI
MITRE by ID	This query viewer displays mitre by id.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/
MITRE by Tactic	This query viewer displays mitre by tactic.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/

Rules

The following table lists all the rules.

Security Monitoring - Base Rule Resources

Resource	Description	URI
Track Rules with MITRE ID	This rule tracks correlation events, where the device custom string 6 label is MITRE ID.	/All Rules/Real-time Rules/

Reports

The following table lists all the reports.

Security Monitoring - Base Report Resources

Resource	Description	URI
MITRE ATT&CK Summary	This report displays a summary of MITRE ATT&CK events by MITRE ID, Tactic, and Rule.	/All Reports/ArcSight Foundation/MITRE ATT&CK/

Use Cases

The following table lists all the use cases.

Security Monitoring - Base Use Case Resources

Resource	Description	URI
MITRE ATT&CK Overview	This use case contains resource for MITRE ATT&CK	/All Use Cases/ArcSight Foundation/Mitre Att&ck Overview/

Security Monitoring - Base - Active Lists Resources By Type

This section lists all Security Monitoring - Base - Active Lists Resources by type.

- [Active Lists](#)147
- [Packages](#)148

Active Lists

The following table lists all the active lists.

Security Monitoring - Base - Active Lists Resources

Resource	Description	URI
Privilege User Groups	This active list should be populated with the user groups that have administrative privileges in your domain. Entries in this list should be in upper case according to the formats given below: <ul style="list-style-type: none"> domain\group example EMEA\ADMINS builtin\group example BUILTIN\ADMINISTRATORS 	/All Active Lists/ArcSight Foundation/Common/
Indicator Types	This list is in sync with Suspicious Indicator Types that are maintained by two lightweight rules.	/All Active Lists/ArcSight Foundation/Common/
Interzone Communications to Restricted Services	This active list contains restricted services.	/All Active Lists/ArcSight Foundation/Common/
Suspicious Indicator Types	This active list contains indicator type that can trigger certain rule.	/All Active Lists/ArcSight Foundation/Common/
Suspicious Countries	This active list contains suspicious countries. For example, ITAR prohibited countries.	/All Active Lists/ArcSight Foundation/Common/
Cleartext Protocols	This active list contains Cleartext Protocols.	/All Active Lists/ArcSight Foundation/Common/
Privilege User Account	This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in upper case, if it is not case sensitive.	/All Active Lists/ArcSight Foundation/Common/
MITRE ATT&CK List	This active list contains MITRE ATT&CK information.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/
Category for Exploit	This active list stores categories for exploit.	/All Active Lists/ArcSight Foundation/Common/

Packages

The following table lists all the packages.

Security Monitoring - Base - Active Lists Package Resources

Resource	Description	URI
Security Monitoring - Base - Active Lists	This package contains pre-defined active list required by Security Monitoring - Base .	/All Packages/ArcSight Foundation/Security Monitoring - Base - Active Lists/

Threat Intelligence Platform Resources By Type

This section lists all Threat Intelligence Platform Resources by type.

• Filters	150
• Fields	151
• Active Lists	158
• Integration Commands	160
• Integration Configurations	161
• Packages	162
• Rules	163
• Dashboards	166
• Queries	167
• Query Viewers	168
• Use Cases	169

Filters

The following table lists all the filters.

Threat Intelligence Platform Filter Resources

Resource	Description	URI
Destination in Suspicious Domain List	This filter identifies the destination domain in the Suspicious Domain List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Destination in Suspicious Address List	This filter identifies the destination address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Source in Suspicious Address List	This filter identifies the source address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Destination in Suspicious Domain	This filter detects all the events, for which the destination is in the suspicious or additional domain list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/

Fields

The following table lists all the fields.

Threat Intelligence Platform Field Resources

Resource	Description	URI
dstAdditionalDomainLevel4	This variable retrieves threat metadata defined by user from the Additional Suspicious Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstExceptionDomainLevel2	This variable retrieves exception domain from the Exceptions Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainIndicatorType3	This variable returns third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSrcDomainList	This variable returns the source domain in list format separated by a dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainIndicatorType	This global variable displays Domain Indicator Types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSizeOfDstDomainList	This variable returns the size of the destination domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressIndicatorType	This variable returns an indicator type for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
exceptionFileHashEntry	This variable Retrieves the threat metadata from the Exception Hash based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcExceptionDomainLevel4	This variable retrieves exception domain from Exceptions - Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcSuspiciousListDomainLevel3	This variable retrieves threat metadata from the Suspicious Domain List corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressIndicatorType1	This variable returns first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getDstDomainList	This variable returns the destination domain in list format separated by a dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcSuspiciousListDomainLevel4	This variable retrieves threat metadata from Suspicious Domain List corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcSuspiciousDomainEntry	This variable retrieves the threat metadata from the Suspicious Domain List based on a source, which is a completely qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressReference	This variable returns reference for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAdditionalDomainLevel2	This variable retrieves the threat metadata defined by user from the Additional Suspicious Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
suspiciousFileHashEntry	This variable retrieves the threat metadata from the Suspicious Hash List based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getDstDomainLevel2	This variable returns the two rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getRequestURLDomain	This variable returns the domain from the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSrcDomainLevel1	This variable returns the rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSizeOfSrcDomainList	This variable returns the size of the source domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcAdditionalDomainLevel4	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainReference	This variable returns reference for the destination domain either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstExceptionAddressEntry	This variable retrieves the threat metadata from the Exception Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getDstDomainLevel4	This variable returns the four rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
additionalFileHashEntry	This variable Retrieves the threat metadata from the Additional Suspicious Hash based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstSuspiciousAddressEntry	This variable retrieves the threat metadata from the Suspicious Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressIndicatorType2	This variable returns second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstExceptionDomainLevel3	This variable retrieves exception domain from the Exceptions Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcSuspiciousListDomainLevel2	This variable retrieves threat metadata from the Suspicious Domain List corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAdditionalAddressEntry	This variable retrieves the threat metadata from the Additional Suspicious Addresses List based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSrcDomainLevel3	This variable returns the three rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getDstDomainLevel1	This variable returns the rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainIndicatorType1	This variable returns first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
dstExceptionDomainLevel4	This variable retrieves exception domain from the Exceptions Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstSuspiciousListDomainLevel4	This variable retrieves threat metadata from Suspicious Domain List corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getDstDomainLevel3	This variable returns the three rightmost destination subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcAdditionalAddressEntry	This variable retrieves the threat metadata from the Additional Suspicious Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSrcDomainLevel2	This variable returns the two rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressValue	This variable returns addresses for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainValue	This variable returns Domains for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcExceptionDomainLevel3	This variable retrieves exception domain from Exceptions - Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcAdditionalDomainEntry	This variable returns the entry of a source in the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
dstDomainIndicatorType2	This variable returns second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getSrcDomainLevel4	This variable returns the four rightmost source subdomains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAdditionalDomainEntry	This variable retrieves the threat metadata from the Additional Suspicious Domain List based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressIndicatorType3	This variable returns third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcAdditionalDomainLevel3	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcExceptionAddressEntry	This variable retrieves the threat metadata from the Exception Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcExceptionDomainLevel2	This variable retrieves exception domain from the Exceptions - Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
getHashValue	This variable retrieves the hash value from fields - File Hash and Old File Hash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcAdditionalDomainLevel2	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Field Resources, continued

Resource	Description	URI
srcSuspiciousAddressEntry	This variable retrieves the threat metadata from the Suspicious Addresses List based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAdditionalDomainLevel3	This variable retrieves the threat metadata defined by user from the Additional Suspicious Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
srcExceptionDomainEntry	This variable retrieves the exception domain from the Exceptions - Domain active list based on a source, which is a fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstSuspiciousListDomainLevel3	This variable retrieves threat metadata from the Suspicious Domain List corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstSuspiciousDomainEntry	This variable retrieves the threat metadata from the Suspicious Domain List based on a destination, which is a fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstSuspiciousListDomainLevel2	This variable retrieves the threat metadata from the Suspicious Domain List corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstDomainIndicatorTypeList	This variable returns a list of indicator type separated by a .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstExceptionDomainEntry	This variable retrieves the threat metadata from the Exception Domain List based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/
dstAddressIndicatorTypeList	This variable returns a list of indicator type separated by a .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/

Active Lists

The following table lists all the active lists.

Threat Intelligence Platform Active List Resources

Resource	Description	URI
Exception Addresses	This active list enables you to define IP addresses that should not be considered as suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Addresses List	This active list contains suspicious addresses collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious Domain	This active list enables you to define suspicious domain.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious URL List	This active list contains suspicious url collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Email List	This active list contains suspicious email addresses collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception URL	This active list enables you to define urls that should not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious Email	This active list enables you to define suspicious email.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Internal Domain Found in Suspicious Domains List	This active list stores internal domains that are found in the suspicious domain list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception Hash	This active list enables you to define hash that should not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Domain List	This active list contains suspicious domains collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Internal Address Found in Reputation Data	This list stores internal IP address that is found in the reputation list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious URL	This active list enables you to define suspicious url.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Active List Resources, continued

Resource	Description	URI
Additional Suspicious Hash	This active list enables you to define suspicious hash.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception Email	This active list enables you to define an email that should not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious Addresses	This active list enables you to define suspicious IP addresses.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Hash List	This active list contains suspicious hash collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception Domain	This active list enables you to define domains that should not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/

Integration Commands

The following table lists all the integration commands.

Threat Intelligence Platform Integration Command Resources

Resource	Description	URI
VirusTotal Hash Lookup	This integration command is used to lookup for hash details using VirusTotal.	/All Integration Commands/ArcSight Foundation/Threat Intelligence Platform/

Integration Configurations

The following table lists all the integration configurations.

Threat Intelligence Platform Integration Configuration Resources

Resource	Description	URI
VirusTotal Hash Lookup	This integration configuration is used to configure the VirusTotal Hash lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/Threat Intelligence Platform/

Packages

The following table lists all the packages.

Threat Intelligence Platform Package Resources

Resource	Description	URI
Threat Intelligence Platform	This package contains default content for threat intelligence platform.	/All Packages/ArcSight Foundation/Threat Intelligence Platform/

Rules

The following table lists all the rules.

Threat Intelligence Platform Rule Resources

Resource	Description	URI
Outbound Communication to a Phishing Address	This rule is triggered by outbound traffic to suspicious phishing site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Outbound Communication to a Phishing Domain	This rule is triggered by outbound traffic to suspicious phishing site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Send to Suspicious Email Address	This rule is triggered by sending an email to a suspicious receiver.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
DNS Query to a Suspicious Address	This rule is triggered by outbound suspicious DNS query.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Add Indicator Types	This rule adds indicator type to a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Remove Indicator Types	This rule removes indicator type from a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Outbound Traffic to a Suspicious Domain	This rule is triggered by outbound traffic to a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Inbound Traffic from a Suspicious Domain	This rule is triggered by inbound traffic from a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Internal Destination Address Found in Suspicious Address List	This rule is triggered when the destination address has category protect, which means company internal address, and is found in the reputation list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Inbound Traffic from a Suspicious Address	This rule is triggered by inbound traffic from a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Rule Resources, continued

Resource	Description	URI
Internal Source Domain Found in Suspicious Domain List	This rule is triggered when the source domain has category protect, which means company internal domain, and is found in the suspicious domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Internal Source Address Found in Suspicious Address List	This rule is triggered when the source address has category protect, which means company internal address, and is found in the reputation list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Command and Control Communication to a Suspicious Domain	This rule is triggered by outbound traffic to suspicious command and control domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Outbound Traffic to a Suspicious Address	This rule is triggered by outbound traffic to a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Command and Control Communication to a Suspicious Address	This rule is triggered by outbound traffic to suspicious command and control server.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Dangerous Browsing to a Suspicious Domain	This rule is triggered by outbound web traffic to a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Suspicious File Hash Activity in Host	This rule is triggered by suspicious file hash in host.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Internal Destination Domain Found in Suspicious Domain List	This rule is triggered when the destination domain has category protect, which means company internal domain, and is found in the suspicious domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Ransomware Activity to a Suspicious Address	This rule is triggered by outbound traffic to a suspicious ransomware site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Receive from Suspicious Email	This rule is triggered by email received from suspicious source.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform Rule Resources, continued

Resource	Description	URI
Dangerous Browsing to a Suspicious URL	This rule is triggered by outbound traffic with suspicious URL.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Ransomware Activity to a Suspicious Domain	This rule is triggered by outbound traffic to a suspicious ransomware site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
Dangerous Browsing to a Suspicious Address	This rule is triggered by outbound web traffic to a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/
DNS Query to a Suspicious Domain	This rule triggered by outbound suspicious DNS query.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/

Dashboards

The following table lists all the dashboards.

Threat Intelligence Platform Dashboard Resources

Resource	Description	URI
Reputation Data Overview	This dashboard displays reputation data overview.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/

Queries

The following table lists all the queries.

Threat Intelligence Platform Query Resources

Resource	Description	URI
Suspicious Hash by Indicator Type	This query selects indicator type and counts from the suspicious hash list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Domain by Indicator Type	This query selects indicator type and counts from the suspicious domain list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Address by Indicator Type	This query selects indicator type and counts from the suspicious address list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious URL by Indicator Type	This query selects indicator type and counts from suspicious url list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/

Query Viewers

The following table lists all the query viewers.

Threat Intelligence Platform Query Viewer Resources

Resource	Description	URI
Top Indicator Type in Suspicious Hash	This query viewer displays the top indicator type in the suspicious hash list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious URL	This query viewer displays the top indicator type in the suspicious url list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious Domain	This query viewer displays the top indicator type in the suspicious domain list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious Address	This query viewer display top indicator type in suspicious address list	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/

Use Cases

The following table lists all the use cases.

Threat Intelligence Platform Use Case Resources

Resource	Description	URI
Threat Intelligence Platform	This use case detects threat based on intelligence data collected from MISP.	/All Use Cases/ArcSight Foundation/Threat Intelligence Platform/

Common Resources By Type

This section lists all Common Resources by type. The resources listed here are part of the /ArcSight Foundation/Shared Libraries/ packages that are automatically installed with ESM.

- [Conditional Variable Filters](#)170
- [Network Filters](#)179
- [Variables Library Fields](#)180

Conditional Variable Filters

The following table lists all the filters.

Conditional Variable Filters

Resource	Description	URI
All Device Information is NULL	This filter identifies events in which there is no device information, meaning that the device vendor, device product, and device version fields are all NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
All Protocol Information is NULL	This filter identifies events in which there is no protocol information (the transport protocol, application protocol, and target port fields are all NULL).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
All Receivers EPS	This filter identifies events in which the device event category is /Monitor/Receiver/All/EPS or /Monitor/Receiver/EPS/All.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Application Protocol is not NULL	This filter identifies if an event has an entry for the Application Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Application Protocol is NULL	This filter identifies if the event target has an application protocol associated with it.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Attacker Address is NULL	This variable identifies events in which the attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Asset has Criticality	This filter identifies events in which the attacker asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Asset has OS Categorization	This filter identifies if the attacker in an event has an asset category in /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/

Conditional Variable Filters, continued

Resource	Description	URI
Attacker Asset ID is NULL	This filter is used by variables to determine if an event has an attacker asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
Attacker Asset Information is NULL	This filter identifies if an event has any attacker asset information. This information consists of the attacker zone, attacker asset name, and attacker address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Host Name is NULL	This filter is used by variables to identify events in which the attacker host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Information is NULL	This filter identifies events in which the attacker zone, attacker host name, and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Port is NULL	This variable identifies events in which the attacker port field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker User ID is NULL	This filter identifies events where the Attacker User ID is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker User Name and ID are NULL	This filter identifies events in which the Attacker User Name and Attacker User ID are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker User Name is NULL	This filter identifies events where the Attacker User Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Attacker Zone AND Address are NULL	This filter identifies events in which the attacker zone and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both an attacker zone and an attacker asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Zone AND Asset Name are NULL	This filter is used by variables to determine if an event has neither an attacker zone or an attacker asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Attacker Zone AND Host are NULL	This filter identifies events in which the attacker zone and attacker address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Attacker Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the attacker zone or attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone is NULL	This filter identifies events in which the attacker zone field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone OR Address is NULL	This filter identifies events where the attacker zone or attacker address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Attacker Zone OR Host is NULL	This filter identifies events in which either the attacker zone or attacker host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Bytes In is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Bytes In is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Bytes Out is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Bytes Out is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Case File Type	This filter identifies events in which the File Type field is Case.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Database Events	This filter identifies events in which the category object is /Host/Application/Database.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Device Address is NULL	This filter is used by variables to identify events in which the device address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Asset has Criticality	This filter identifies events in which the device asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Asset has OS Categorization	This filter identifies if the device in an event has an asset category in /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Asset ID is NULL	This filter is used by variables to determine if an event has an device asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/

Conditional Variable Filters, continued

Resource	Description	URI
Device Asset Information is NULL	This filter is used by variables to determine if an event has any device asset information. This information consists of the device zone, device asset name, and device address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Vendor AND Product are NULL	This filter identifies events in which the device vendor and device product fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor OR Product is NULL	This filter identifies events in which the device vendor or device product field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Version is NULL	This filter identifies events in which the device product field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Zone AND Address are NULL	This variable is used by variables to identify events in which the device zone and device address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both an device zone and an device asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Zone AND Asset Name are NULL	This filter identifies if an event has neither a device zone or an device asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Device Zone OR Address is NULL	This filter is used by variables to identify events in which the device zone or device address field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Double-digit Julian Day	This filter supports the variable Julian Day by checking the end time for a double digit day. The Julian Day variable prepends 0 or 00 to days with a single Julian digit, so that the format is always DDD (for example, January 1st displays as 001 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Email Address in Attacker User ID	This filter identifies events in which the attacker user ID field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Email Address in Attacker User Name	This filter identifies events in which the attacker user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Email Address in Target User ID	This filter identifies events in which the target user ID field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/

Conditional Variable Filters, continued

Resource	Description	URI
Email Address in Target User Name	This filter identifies events in which the target user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has Actor by Account Information	This filter identifies events in which the global variable ActorByAccountID returns actor information.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has Actor by Custom Account Information	This filter identifies events in which the global variable ActorByCustomFields returns actor information.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Event Has E-mail Address	This filter identifies events in which one or more user ID or user name field has an email address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Firewall Events	This filter retrieves events with the Firewall category device group.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Inbound Network	This filter identifies events in which the device event category ends with /In.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Notification Event has Acknowledgement Status	This filter identifies notification events that have a Device Custom String 6 label set as Acknowledgement Status.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Configuration Resource	This filter identifies notification events that have a Device Custom String 2 label set as Configuration Resource.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/
Notification Event has Destination Group	This filter identifies notification events that have a Device Custom String 4 label set as Group.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/

Conditional Variable Filters, continued

Resource	Description	URI
Notification Event has Rule Name	This filter identifies notification events that have a Device Custom String 3 label set as Rule Name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has User Name	This filter identifies notification events that have an attacker user name to represent the user who acknowledged or resolved a notification.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Operating System Events	This filter identifies events in which the category device group is Operating System.	/All Filters/ArcSight Foundation/Common/Device Class Filters/
Remaining Disk Less than 5 Percent	This filter identifies events in which the remaining disk space is less than five percent.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Remaining Disk More than 10 Percent	This filter identifies events in which the remaining disk space is greater than ten percent.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/
Sensor Type is CPU	This filter identifies events in which the sensor type is CPU.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/Sensor Type is CPU
Sensor Type is FAN	This filter identifies events in which the sensor type is FAN.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/ArcSight Appliance/Sensor Type is FAN
Single-digit Day	This filter identifies the Day variable by checking the end time to see if it is a single or double digit day. The Day variable prepends 0 to days with a single digit, so that the format is always DD (for example, the 1st displays as 01 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Day
Single-digit Hour	This filter supports the Hour variable by checking the end time to see if it is a single or double digit hour. The Hour variable prepends 0 to hours with a single digit, so that the format is always HH (for example, 7:00 displays as 07 instead of 7).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Hour

Conditional Variable Filters, continued

Resource	Description	URI
Single-digit Julian Day	This filter supports the Julian Day variable by checking the end time for a double digit day. The Julian Day variable prepends 0 or 00 to days with a single Julian digit, so that the format is always DDD (for example, January 1st displays as 001 instead of 1).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Julian Day
Single-digit Minute	This filter supports the Minute variable by checking the end time to see if it is a single or double digit minute. The Minute variable prepends 0 to minutes with a single digit, so that the format is always mm.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Minute
Single-digit Month	This filter supports the Month variable by checking the end time to see if it is a single or double digit month. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/Single-digit Month
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/Target Address is NULL
Target Asset has Application Categorization	This filter identifies if the target of an event has an Asset Category in /Site Asset Categories/Application.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
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.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset has Criticality	This filter identifies events in which the target asset is categorized under /All Asset Categories/System Asset Categories/Criticality.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset has OS Categorization	This filter identifies if the target in an event has an Asset Category within /Site Asset Categories/Operating System.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset ID is NULL	This filter determines if an event has a target asset ID.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Asset Information is NULL	This filter is used by variables to determine if an event has any target asset information. This information consists of the target zone, target asset name, and target address.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Target Information is NULL	This filter identifies events in which the target zone, target host name, and target address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Object starts with Host Application	This filter identifies if an event Category Object is within /Host/Application.	/All Filters/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.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Target Port is NULL	This filter is used by variables to check if the event target has a port number associated with it.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Target Service Name is not NULL	This filter identifies if an event has an entry for the Target Service Name field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
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.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target User Name and ID are NULL	This filter identifies events in which the Target User Name and Target User ID are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target User Name is NULL	This filter identifies events where the Target User Name is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/User/
Target Zone AND Address are NULL	This filter identifies events in which the target zone and target address fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Asset Name are NOT NULL	This filter is used by variables to determine if an event has both a target zone and a target asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Zone AND Asset Name are NULL	This filter determines if an event has neither a target zone or a target asset name.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Asset/
Target Zone AND Host are NULL	This filter identifies events in which the target zone and target host name fields are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the target zone or target address field is NULL, but not both.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/

Conditional Variable Filters, continued

Resource	Description	URI
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone OR Address is NULL	This filter identifies events in which the target zone or target address field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Zone OR Host is NULL	This filter identifies events in which either the target zone or target host name field is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Host/
Transport AND Application Protocols are NULL	This filter is used by variables to identify events in which the transport and application protocols are NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport OR Application Protocol is NULL	This variable identifies events in which either the transport protocol or the application protocol is NULL.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport Protocol is not NULL	This filter identifies if an event has an entry for the Transport Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
Transport Protocol is NULL	This filter is used by variables to determine if an event has an entry for the Transport Protocol field.	/All Filters/ArcSight Foundation/Common/Conditional Variable Filters/Protocol/
VPN Events	This filter identifies events in which the category device group is VPN.	/All Filters/ArcSight Foundation/Common/Device Class Filters/

Network Filters

The following tables list all the filters.

Network Filters Resources

Resource	Description	URI
External Source	This filter identifies events originating from outside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
External Target	This filter identifies events targeting the outside network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
External to External Events	This filter identifies events external to the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Internal Source	This filter identifies events coming from inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal to Internal Events	This filter retrieves events internal to the company network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	/All Filters/ArcSight Foundation/Common/Network Filters/Location Filters/

Variables Library Fields

The following table lists all the global variable fields.

Global Variable Fields

Resource	Description	URI
ActingSystem	This variable returns the attacker host (if known) or the target host if it is the only host information available within the event. The format is the same as the AttackerHost or TargetHost variable.	/All Fields/ArcSight Foundation/Variables Library/Host Information/
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.	/All Fields/ArcSight Foundation/Variables Library/User Information/
Agent IPv6 Address	This variable is an alias for Device Custom IPv6 Address4.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
Attacker IPv6 Address	This field denotes the Attacker IPv6 address. The term attacker is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Source, return Device Custom IPv6 Address1 (aliased as Source IPv6 Address), or return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address)	/All Fields/ArcSight Foundation/Variables Library/IPv6/
AttackerAsset	This variable returns the attacker asset information from an event. The asset information is in the format <attackerZoneName>. <attackerAssetName> <attackerAddress> Examples: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30 unknown	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
AttackerAssetCriticality	This variable returns the criticality categorization of the attacker asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (Very High, High, Medium, Low, Very Low, or unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
AttackerHost	This variable returns available attacker information from an event. The format of the information is: <attackerZoneName>. <attackerHostName> <attackerAddress>:<attackerPort>. Information that is not in the event does not show a place-holder. For example: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown	/All Fields/ArcSight Foundation/Variables Library/Host Information/

Global Variable Fields, continued

Resource	Description	URI
AttackerOS	This variable returns the operating system of the attacker asset (if available) or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset 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.	/All Fields/ArcSight Foundation/Variables Library/User Information/
DateTime	This variable returns the date and time in the year/month/day-hour:minute format. For example: 2009/10/03-00:43	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
DateValue	This variable returns the date in the year/month/day format. For example: 2009/10/03.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Day	This variable returns the day in a two-digit format. For example: 03	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
DayOfWeek	This variable returns the day of the week, spelled out. When using this variable in a query, do not use it for sorting, as the sort will be alphabetical on the name of the day, not the order of the days in the week.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Destination IPv6 Address	This variable is an alias for Device Custom IPv6 Address2.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
Device IPv6 Address	This variable is an alias for Device Custom IPv6 Address3.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
DeviceAsset	This variable returns the device asset information from an event. The asset information is in the format: <deviceZoneName>. <deviceAssetName> <deviceAddress>. For example: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30 unknown	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
DeviceAssetCriticality	This variable returns the criticality categorization of the device asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (for example, Very High, High, Medium, Low, Very Low, unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/

Global Variable Fields, continued

Resource	Description	URI
DeviceInfo	This variable returns the device information, including the device vendor, the device product, and the device version, if available within the event. The format is deviceVendor. <deviceProduct> or <deviceVendor> <deviceProduct> v. <deviceVersion>	/All Fields/ArcSight Foundation/Variables Library/
DeviceOS	This variable returns the operating system of the device asset (if available) or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
EndTimeValue	This variable returns the hour and minute in the hour:minute format. For example: 00:10	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
GBytesIn	This variable converts the Bytes In field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example when Bytes In < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesIn_Labeled	This variable converts the Bytes In field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000,000, the result is 0). It is then converted to a string, and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesOut	This variable converts the Bytes Out field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesOut_Labeled	This variable converts the Bytes Out field to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000,000, the result is 0). It is then converted to a string, and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example when Bytes In + Bytes Out < 10,000,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
GBytesTotal_Labeled	This variable converts the combination of the Bytes In and Bytes Out fields to GBytes, where a GByte is defined as 1,000,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000,000, the result is 0). It is then converted to a string and labeled with the suffix GB (for example, 0.01 GB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
GetEmailAddress	This variable does a simple check on the target user name, target user ID, attacker user name, and attacker user ID fields to display the email address. The precedence is attacker user name, then attacker user ID, then target user name, then finally, target user ID, (if all fields have an email address, the attacker user name is the one returned).	/All Fields/ArcSight Foundation/Variables Library/User Information/
Hour	This variable returns the hour in a two-digit format. For example: 02	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDate	This variable returns the date and time in the year/julian day format. For example: 2009/003, 2010/084, or 2007/363.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDateTime	This variable returns the date and time in the year/julian day-hour:minute format. For example: 2009/003-00:53, 2010/084-08:00, 2007/363-15:45.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
JulianDay	This variable returns the day in a three-digit, julian day format. For example, 003, 084, 363.	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
KBytesIn	This variable converts the Bytes In field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesIn_Labeled	This variable converts the Bytes In field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (when Bytes In < 10, the result will be 0). It is then converted to a string, and labeled with the suffix KB (such as, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesOut	This variable converts the Bytes Out field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
KBytesOut_Labeled	This variable converts the Bytes Out field to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10, the result is 0). It is then converted to a string, and labeled with the suffix KB (for example, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (when Bytes In + Bytes Out < 10, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
KBytesTotal_Labeled	This variable converts the combination of the Bytes In and Bytes Out fields to KBytes, where a KByte is defined as 1,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In+ Bytes Out < 10, the result is 0). It is then converted to a string, and labeled with the suffix KB (for example, 0.01 KB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesIn	This variable converts the Bytes In field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesIn_Labeled	This variable converts the Bytes In field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesOut	This variable converts the Bytes Out field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesOut_Labeled	This variable converts the Bytes Out field to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes Out < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
MBytesTotal	This variable converts the combination of the Bytes In and Bytes Out fields to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000, the result is 0).	/All Fields/ArcSight Foundation/Variables Library/Bytes/

Global Variable Fields, continued

Resource	Description	URI
MBytesTotal_Labeled	This variable converts the combination of Bytes In and Bytes Out fields to MBytes, where a MByte is defined as 1,000,000 bytes. The value is set to have no more than two digits past the decimal point, so that 0.01 is the smallest non-zero value returned (for example, when Bytes In + Bytes Out < 10,000, the result is 0). It is then converted to a string, and labeled with the suffix MB (for example, 0.01 MB).	/All Fields/ArcSight Foundation/Variables Library/Bytes/
Minute	This variable returns the minute in a two-digit format. For example: 02	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Month	This variable returns the numeric value of the month from the end time date field. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/
Protocol	This variable returns the available protocol information within the event. The format is <transportProtocol> <applicationProtocol>(targetPort) Examples: TCP HTTP(80) TCP(1024) ICMP DNS(53) unknown	/All Fields/ArcSight Foundation/Variables Library/
Source IPv6 Address	This variable is an alias for Device Custom IPv6 Address1.	/All Fields/ArcSight Foundation/Variables Library/IPv6/
SystemActedUpon	This variable returns the target host (if known) or the attacker host if it is the only host information available within the event. The format is the same as the TargetHost or AttackerHost variables.	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
Target IPv6 Address	This field denotes the Target IPv6 address. The term target is dependent upon the originator field, i.e., Source or Destination, depending on the specific event. If the originator field is Destination, return Device Custom IPv6 Address2 (aliased as Destination IPv6 Address), or return Device Custom IPv6 Address1 (aliased as Source IPv6 Address)	/All Fields/ArcSight Foundation/Variables Library/IPv6/
TargetAsset	This variable returns the target asset information from an event. The asset information is in the format <targetZoneName> <targetAssetName> <targetAddress> Examples: RFC1918: 192.168.0.0-192.168.255.255, Itwiki.sv.arcsight.com 192.168.10.20 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30 unknown	/All Fields/ArcSight Foundation/Variables Library/Asset Information/
TargetAssetCriticality	This variable returns the criticality categorization of the target asset as categorized using the /All Asset Categories/System Asset Categories/Criticality asset categories (for example, Very High, High, Medium, Low, Very Low, unknown).	/All Fields/ArcSight Foundation/Variables Library/Asset Information/

Global Variable Fields, continued

Resource	Description	URI
TargetHost	This variable returns available target information from an event. The format of the information is targetZoneName. <targetHostName> <targetAddress>:<targetPort> Information that is not in the event will not show a place-holder. Examples: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown	/All Fields/ArcSight Foundation/Variables Library/Host Information/
TargetOS	This variable returns the operating system of the target asset (if available), or unknown. For example: Microsoft/Windows XP, Microsoft/Windows 2000/Server, Unknown.	/All Fields/ArcSight Foundation/Variables Library/Asset 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.	/All Fields/ArcSight Foundation/Variables Library/User Information/
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	/All Fields/ArcSight Foundation/Variables Library/Bytes/
UserActedUpon	This variable selects the target user (if known) or the attacker user if it is the only user information available within the event. The format is the same as the TargetUser or AttackerUser variable.	/All Fields/ArcSight Foundation/Variables Library/User Information/
Year	This variable returns the year. For example: 2002	/All Fields/ArcSight Foundation/Variables Library/Timestamp Formats/

ArcSight System Resources

This chapter lists all the resources by type in the ArcSight System packages.

- [Active Channels](#) 187
- [Active Lists](#) 188
- [Destinations](#) 189
- [Field Sets](#) 190
- [Filters](#) 192
- [Integration Commands](#) 196
- [Integration Configurations](#) 197
- [Queries](#) 199
- [Reports](#) 200
- [Rules](#) 201

Active Channels

The following table lists all the active channels.

Active Channel Resources

Resource	Description	URI
Last 5 Minutes	This active channel shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.	/All Active Channels/ArcSight System/All Events/
Last Hour	This active channel shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data.	/All Active Channels/ArcSight System/All Events/
Live	This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	/All Active Channels/ArcSight System/Core/

Active Channel Resources, continued

Resource	Description	URI
Personal Live	This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events. This active channel also hides all the events that have been assigned to the current user.	/All Active Channels/ArcSight System/Core/
System Events Last Hour	This active channel shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlated events.	/All Active Channels/ArcSight System/
Today	This active channel shows events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	/All Active Channels/ArcSight System/

Active Lists

The following table lists all the active lists.

Active List Resources

Resource	Description	URI
Account Authenticators	This active list is used by the actor global variables to determine the Identity Management authenticator, based on the event, so that an actor can be determined from event information.	/All Active Lists/ArcSight System/Actor Data Support/
Compromised List	This active list contains hosts that may have been compromised by an attack.	/All Active Lists/ArcSight System/Threat Tracking/
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	/All Active Lists/ArcSight System/Tuning/
Hit List	This active list contains hosts targeted by a potential attacker.	/All Active Lists/ArcSight System/Targets/
Hostile List	This active list contains hosts that have been attempting attacks on systems.	/All Active Lists/ArcSight System/Threat Tracking/

Active List Resources, continued

Resource	Description	URI
Infiltrators List	This active list contains hosts which have compromised (infiltrated) a system.	/All Active Lists/ArcSight System/Threat Tracking/
Reconnaissance List	This active list contains IP addresses of hosts which have performed reconnaissance activity.	/All Active Lists/ArcSight System/Threat Tracking/
Scanned List	This active list contains hosts that have been scanned by a potential attacker.	/All Active Lists/ArcSight System/Targets/
Suspicious List	This active list contains hosts which have performed suspicious activity, either on the local system or over the network.	/All Active Lists/ArcSight System/Threat Tracking/
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	/All Active Lists/ArcSight System/Attackers/
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	/All Active Lists/ArcSight System/Attackers/
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.	/All Active Lists/ArcSight System/Tuning/

Destinations

The following table lists all the destinations.

Destination Resources

Resource	Description	URI
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	/All Destinations/SOC Operators/1/
admincert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	/All DestinationsCERT Team/1/

Field Sets

The following table lists all the field sets.

Field Set Resources

Resource	Description	URI
Actor Base	This field set contains all the fields related to actors.	/All Field Sets/ArcSight System/Actor Field Sets
Actor Information	This field set contains a set of fields used to view actor data in events.	/All Field Sets/ArcSight System/Actor Field Sets
Asset Information	This field set contains a collection of fields used to view asset data in asset channels, queries, and so on, focusing on asset resources.	/All Field Sets/ArcSight System/Asset Field Sets
Case Information	This field set contains a collection of fields used to view case attributes in case channels, queries, and so on, focusing on case resources.	/All Field Sets/ArcSight System/Case Field Sets
Event Base	This field set contains all the ESM event fields.	/All Field Sets/ArcSight System/Event Field Sets
Annotation	This field set contains annotation attributes for events.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Annotation-MgrRcpt	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
ArcSight Admin	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Assets	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Categories	This field set shows all the categorization fields for events.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Executive	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels

Field Set Resources, continued

Resource	Description	URI
Export	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
MSSP	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Security	This field set contains several fields that are formatted to show more detailed information for security-related fields without needing to use the event inspector.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Standard- MgrRcpt	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Super Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
Annotation	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Categories	This field set shows all the categorization fields for events.	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Common Conditions Editor	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Event Inspector	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
Rule Action - Set Event Field	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit

Field Set Resources, continued

Resource	Description	URI
Super Minimal	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
TurboMode Comprehensive	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit
TurboMode Fastest	None	/All Field Sets/ArcSight System/Event Field Sets/Inspect - Edit

Filters

The following table lists all the filters.

Filter Resources

Resource	Description	URI
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	/All Filters/ArcSight System/Event Types/
All Events	This filter matches all events.	/All Filters/ArcSight System/Core/
ArcSight Correlation Events	This filter identifies correlation events generated by ArcSight systems.	/All Filters/ArcSight System/Event Types/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	/All Filters/ArcSight System/Event Types/
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	/All Filters/ArcSight System/Event Types/
Attacker User Name is NULL	This filter identifies events in which the attacker user name is NULL.	/All Filters/ArcSight System/Core/

Filter Resources, continued

Resource	Description	URI
Attackers on Hostile List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	ArcSight System/Core/Threat Level Filters/
Attackers on Infiltrators List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Attackers on Reconnaissance List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Attackers on Suspicious List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Blocked ArcSight Internal Events	This filter is applied to audit events before they are inserted. Modify this filter to disable internal events as needed.	/All Filters/ArcSight System/Event Types/
Compromised Targets	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.	/All Filters/ArcSight System/Core/Threat Level Filters/
Connector Asset Auto-Creation Controller	This filter is used internally by the asset auto-creation feature for connectors. The asset auto-creation feature automatically creates assets in the ArcSight Asset model for events whose connectors are not already modeled. You can configure the filter to include or exclude connectors from the asset auto-creation feature.	/All Filters/ArcSight System/Asset Auto-Creation/
Correlation Events	This filter identifies correlation events.	/All Filters/ArcSight System/Event Types/
Device Asset Auto-Creation Controller	This filter is used internally by the asset auto-creation feature for devices. The asset auto-creation feature automatically creates assets in the ArcSight Asset model for events whose devices are not already modeled. You can configure the filter to include or exclude devices from the asset auto-creation feature.	/All Filters/ArcSight System/Asset Auto-Creation/
High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a High criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/

Filter Resources, continued

Resource	Description	URI
Low Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Low criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Medium Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Medium criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
No Events	This is a utility filter that does not match any events passing through the system.	/All Filters/ArcSight System/Core/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	/All Filters/ArcSight System/Event Types/
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	/All Filters/ArcSight System/Event Types/
Non-Categorized Events	This filter selects events that have no categorization.	/All Filters/ArcSight System/Event Types/
Not Correlated and Not Closed	This filter selects events that have not had their event annotation flags set to correlated (by a rule) or close (by an analyst).	/All Filters/ArcSight System/Event Types/
Not Correlated and Not Closed and Not Hidden	This filter selects events that have not had their event annotation flags set to correlated (by a rule), close (by an analyst) or hidden (by system settings).	/All Filters/ArcSight System/Event Types/
SNMP Trap Sender	This resource has no description.	/All Filters/ArcSight System/SNMP Forwarding/
Severity High	This filter captures events where the agent severity is High.	/All Filters/ArcSight System/Event Types/
Severity Low	This filter captures events where the agent severity is Low.	/All Filters/ArcSight System/Event Types/

Filter Resources, continued

Resource	Description	URI
Severity Medium	This filter captures events where the agent severity is Medium.	/All Filters/ArcSight System/Event Types/
Severity Unknown	This filter captures events where the agent severity is either NULL or Unknown.	/All Filters/ArcSight System/Event Types/
Severity Very High	This filter captures events where the agent severity is Very High.	/All Filters/ArcSight System/Event Types/
Target Asset Scanned for Open Ports	This filter detects events in which the Target Asset ID is categorized as scanned and showing open ports. This filter is used by the Priority Formula.	/All Filters/ArcSight System/Core/
Target Asset Scanned for Vulnerabilities	This filter detects events in which the Target Asset ID is categorized as scanned and showing vulnerabilities. This filter is used by the Priority Formula.	/All Filters/ArcSight System/Core/
Unknown Criticality Assets	This filter captures events where the target asset ID exists but has been categorized as having criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Very High Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very High criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/
Very Low Criticality Assets	This filter captures events where the target asset ID has been categorized as having a Very Low criticality.	/All Filters/ArcSight System/Core/Threat Level Filters/

Integration Commands

The following table lists all the integration commands.

Integration Command Resources

Resource	Description	URI
Web Search	This integration command is used to run a search with the selected item, device vendor, and device product in the selected event.	/All Integration Commands/ArcSight System/Tools/
Nslookup (Linux)	This integration command is used to find details about the Domain Name System (DNS). Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Nslookup-IPv6 (Linux)	This integration command is used to find details about an IPv6 hostname in the Domain Name System (DNS). Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Ping (Linux)	This integration command is used to test whether a particular host is reachable across an IP network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Ping6 (Linux)	This integration command is used to test whether a particular host is reachable across an IPv6 network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Portinfo (Linux)	This integration command is used to find information about the selected port. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Traceroute (Linux)	This integration command is used to determine the route taken by packets across an IP network. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Whois (Linux)	This integration command is used to determine the owner of a domain name or an IP address on the Internet. Run this command from a Linux console.	/All Integration Commands/ArcSight System/Tools/Linux/
Nslookup (Windows)	This integration command is used to find details about the Domain Name System (DNS). Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Ping (Windows)	This integration command is used to test whether a particular host is reachable across an IP network. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/

Integration Command Resources, continued

Resource	Description	URI
Portinfo (Windows)	This integration command is used to find information about the selected port. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Traceroute (Windows)	This integration command is used to determine the route taken by packets across an IP network. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/
Whois (Windows)	This integration command is used to determine the owner of a domain name or an IP address on the Internet. Run this command from a Windows console.	/All Integration Commands/ArcSight System/Tools/Windows/

Integration Configurations

The following table lists all the integration configurations.

Integration Configuration Resources

Resource	Description	URI
Web Search	This integration configuration is used to configure the web search command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight System/Tools/
Nslookup (Linux)	This integration configuration is used to configure the Linux nslookup command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Nslookup- IPv6 (Linux)	This integration configuration is used to configure the Linux nslookup command. You can run the command on an IPv6 address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Ping (Linux)	This integration configuration is used to configure the Linux ping command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Ping6 (Linux)	This integration configuration is used to configure the Linux ping command. You can run the command on an IPv6 address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Portinfo (Linux)	This integration configuration is used to configure the Linux portinfo command. You can run the command on a port (Integer) selected in the viewer or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/

Integration Configuration Resources, continued

Resource	Description	URI
Traceroute (Linux)	This integration configuration is used to configure the Linux traceroute command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Whois (Linux)	This integration configuration is used to configure the Linux whois command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Linux/
Nslookup (Windows)	This integration configuration is used to configure the Windows nslookup command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Ping (Windows)	This integration configuration is used to configure the Windows ping command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Portinfo (Windows)	This integration configuration is used to configure the Windows portinfo command. You can run the command on a port (Integer) selected in the viewer or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Traceroute (Windows)	This integration configuration is used to configure the Windows traceroute command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/
Whois (Windows)	This integration configuration is used to configure the Windows whois command. You can run the command on an IP address or hostname (string) selected in the viewer, on an asset in the navigator, or on a field selected in an editor such as the event inspector.	/All Integration Configurations/ArcSight System/Tools/Windows/

Queries

The following table lists all the queries.

Query Resources

Resource	Description	URI
Actor Event Count by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Custom Fields	This query shows activity related to an actor based on the AccountByCustomFields global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Event Count by Target Username	This query shows activity related to an actor based on the AccountByTargetUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Custom Fields	This query shows activity related to an actor based on the ActorByCustomFields global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Events by Target Username	This query shows activity related to an actor based on the ActorByTargetUsername global variable.	/All Queries/ArcSight System/Core/Actor Context Report/
Actor Information	This query shows activity related to an actor.	/All Queries/ArcSight System/Core/Actor Context Report/
Selected Case Query	This query returns information for the selected case. The query must contain a single parameter for the case resource ID.	/All Queries/ArcSight System/Core/Selected Case Report/

Reports

The following table lists all the reports.

Report Resources

Resource	Description	URI
Actor Context Report by Account ID	This report shows activity related to an actor based on the ActorByAccountID global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Attacker Username	This report shows activity related to an actor based on the ActorByAttackerUserName global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Custom Fields	This report shows activity related to an actor based on the ActorByCustomFields global variable.	/All Reports/ArcSight System/Core/
Actor Context Report by Target Username	This report shows activity related to an actor based on the ActorByTargetUserName global variable.	/All Reports/ArcSight System/Core/
Assets having Vulnerability	This report is used by the ArcSight console for internal processing, and is not meant to be run on its own.	/All Reports/ArcSight System/Core/
Selected Case Report	This report shows information for the selected case.	/All Reports/ArcSight System/Core/
Vulnerabilities of an Asset	This report is used by the ArcSight console for internal processing, and is not meant to be run on its own.	/All Reports/ArcSight System/Core/

Rules

The following table lists all the rules.

Rule Resources

Resource	Description	URI
Compromise - Attempt	This rule detects any attempt to compromise a device from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/
Compromise - Success	This rule detects any successful attempt to compromise a device from a source that is not listed in a trusted active list, with either the attacker information (zone and address) or the target information present. The rule triggers whenever an event is categorized as Success and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List and Infiltrators List active lists, and the target address is added to the Compromised List and Hit List active lists.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/
Hostile - Attempt	This rule detects any hostile attempt on a device that is not already compromised from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Hostile, and the target does not belong to a compromised active list. On the first event, agent severity is set to medium, attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Hostile/
Hostile - Success	This rule detects any successful hostile attempts on a device that is not already compromised from a source not listed in a trusted active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Hostile/

Rule Resources, continued

Resource	Description	URI
Incident Resolved - Remove From List	This rule detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. Note: This rule triggers only if you have the Intrusion Monitoring package installed from a previous ESM release.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Compromise/
Reconnaissance - Attackers	The rule identifies correlation events which originate from other reconnaissance rules. The events signify successful reconnaissance events from an attacker which is added to the Reconnaissance ActiveList.	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Reconnaissance/
Reconnaissance - Targets	The rule identifies correlation events which originate from other reconnaissance rules. The events signify successful reconnaissance events targetted by an external attacker to an internal asset. The rule adds the target information into the Scanned ActiveList	/All Rules/Real-Time Rules/ArcSight System/Threat Tracking/Reconnaissance/

1. ArcSight ESM Standard Content Guide Foundation Resources	2
1.1 Security Monitoring - Base 2.0 Resources By Type	2
1.1.1 Security Monitoring - Base 2.0 Active Channels	2
1.1.2 Security Monitoring - Base 2.0 Active Lists	2
1.1.3 Security Monitoring - Base 2.0 Dashboards	2
1.1.4 Security Monitoring - Base 2.0 Data Monitors	3
1.1.5 Security Monitoring - Base 2.0 Fields	3
1.1.6 Security Monitoring - Base 2.0 Field Sets	4
1.1.7 Security Monitoring - Base 2.0 Filters	4
1.1.8 Security Monitoring - Base 2.0 Integration Commands	4
1.1.9 Security Monitoring - Base 2.0 Integration Configurations	5
1.1.10 Security Monitoring - Base 2.0 Packages	5
1.1.11 Security Monitoring - Base 2.0 Queries	5
1.1.12 Security Monitoring - Base 2.0 Query Viewers	5
1.1.13 Security Monitoring - Base 2.0 Reports	5
1.1.14 Security Monitoring - Base 2.0 Use Cases	5
1.2 Security Monitoring - Base - Active Lists 2.0 Resources By Type	5
1.2.1 Security Monitoring - Base - Active Lists 2.0 Active Lists	6
1.2.2 Security Monitoring - Base - Active Lists 2.0 Packages	6
1.2.3 Security Monitoring - Base - Active Lists 2.0 Rules	6
1.3 Security Threat Monitoring 2.0 Resources By Type	7
1.3.1 Security Threat Monitoring 2.0 Active Channels	7
1.3.2 Security Threat Monitoring 2.0 Active Lists	7
1.3.3 Security Threat Monitoring 2.0 Dashboards	7
1.3.4 Security Threat Monitoring 2.0 Data Monitors	8
1.3.5 Security Threat Monitoring 2.0 Fields	9
1.3.6 Security Threat Monitoring 2.0 Field Sets	10
1.3.7 Security Threat Monitoring 2.0 Filters	11
1.3.8 Security Threat Monitoring 2.0 Packages	13
1.3.9 Security Threat Monitoring 2.0 Queries	13
1.3.10 Security Threat Monitoring 2.0 Query Viewers	13
1.3.11 Security Threat Monitoring 2.0 Rules	14
1.3.12 Security Threat Monitoring 2.0 Use Cases	23
1.4 Threat Intelligence Platform 2.0 Resources By Type	24
1.4.1 Threat Intelligence Platform 2.0 Active Lists	24
1.4.2 Threat Intelligence Platform 2.0 Dashboards	25
1.4.3 Threat Intelligence Platform 2.0 Fields	25
1.4.4 Threat Intelligence Platform 2.0 Filters	30
1.4.5 Threat Intelligence Platform 2.0 Integration Commands	31
1.4.6 Threat Intelligence Platform 2.0 Integration Configurations	31
1.4.7 Threat Intelligence Platform 2.0 Packages	31
1.4.8 Threat Intelligence Platform 2.0 Queries	31
1.4.9 Threat Intelligence Platform 2.0 Query Viewers	32
1.4.10 Threat Intelligence Platform 2.0 Rules	32
1.4.11 Threat Intelligence Platform 2.0 Use Cases	34

ArcSight ESM Standard Content Guide Foundation Resources

This Appendix lists all the resources by type in the ArcSight Foundation packages.

Security Monitoring - Base 2.0 Resources By Type

This section lists all Security Monitoring - Base 2.0 Resources by type.

Security Monitoring - Base 2.0 Active Channels

The following table lists all the active channels.

Resource	Description	URL
MITRE ATT&CK	This active channel shows all correlation rules with MITRE ATT&CK information.	/All Active Channels/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Active Lists

The following table lists all the active lists.

Resource	Description	URL
Suspicious Activities Tracking	This active list tracks suspicious activities.	/All Active Lists/ArcSight Foundation/Common/
External Device Connected With Autorun	This active list tracks external drives plugged on machines having autorun.inf	/All Active Lists/ArcSight Foundation/Common/
Attacker and Target Based Suppression	This suppression list is based on attacker address, target address, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Tracking Rules Triggered	This active list is used to track all triggered rules.	/All Active Lists/ArcSight Foundation/Common/
MITRE ATT&CK Activity Tracking	This active list tracks MITRE ATT&CK activity.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/
Rules Triggered with MITRE ID	This active list stores MITRE ATT&CK information from correlation rules.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/
Username Based Suppression	This suppression list is based on target username and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Target Based Suppression	This suppression list is based on target address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Target and Username Based Suppression	This suppression list is based on target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Attacker and Target and Username Based Suppression	This suppression list is based on attacker address, target address, target username, and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Attacker Based Suppression	This suppression list is based on attacker address and generator.	/All Active Lists/ArcSight Foundation/Common/Suppression List/
Host Name Based Suppression	This suppression list is based on device host name and generator.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/

Security Monitoring - Base 2.0 Dashboards

The following table lists all the dashboards.

Resource	Description	URL
MITRE ATT&CK Targets Overview	This dashboard provides overview of MITRE ATT&CK events with targets information.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/
MITRE ATT&CK Overview	This dashboard displays MITRE ATT&CK overview.	/All Dashboards/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Data Monitors

The following table lists all the data monitors.

Resource	Description	URL
Top Fired MITRE ATT&CK Rules	This data monitor displays the top five fired rules with MITRE ATT&CK information.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Top Target IPs	This data monitor displays the top five target IP addresses with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
MITRE Attackers and Targets Relations	This data monitor shows the relationship between attacker and target machines using MITRE IDs.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Last MITRE ATT&CK Events	This data monitor displays the last five MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/
Top Target Users	This data monitor displays the top five users with MITRE ATT&CK related events.	/All Data Monitors/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Fields

The following table lists all the fields.

Resource	Description	URL
dc_userName	This variable checks if the target username is null. If the target user name is null, then the source username is entered, otherwise the target username is entered.	/All Fields/ArcSight Foundation/Common/
mitreName	This variable converts the MITRE name from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_srcDnsDomain	This variable returns the source DNS domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_endTimeinHour	This variable returns the hour of end time.	/All Fields/ArcSight Foundation/Common/
serverAddress	This variable returns server address.	/All Fields/ArcSight Foundation/Common/
dc_dvcHostName	This variable returns the device hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_tgtHostName	This variable returns the target hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_dstDnsDomain	This variable returns the destination DNS domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_srcHostName	This variable returns the source hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_atkHostName	This variable returns the attacker hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_dstUserName	This variable returns the destination username in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_tgtDnsDomain	This variable returns the target DNS domain in lowercase.	/All Fields/ArcSight Foundation/Common/
dc_srcUserName	This variable returns the source username in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_serverHostName	This variable returns the server hostname.	/All Fields/ArcSight Foundation/Common/

getMitre	This variable returns MITRE ATT&CK information.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_tgtUserName	This variable returns the target username in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_atkUserName	This variable returns the attacker username in uppercase.	/All Fields/ArcSight Foundation/Common/
dc_atkDnsDomain	This variable returns the attacker DNS domain in lowercase.	/All Fields/ArcSight Foundation/Common/
serverAddressZone	This variable returns the server zone.	/All Fields/ArcSight Foundation/Common/
dc_dstHostName	This variable returns the destination hostname in lowercase.	/All Fields/ArcSight Foundation/Common/
tacticName	This variable converts MITRE tactic from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
mitreID	This variable converts MITRE ID from list to string.	/All Fields/ArcSight Foundation/MITRE ATT&CK/
dc_nullString	This variable returns null string.	/All Fields/ArcSight Foundation/Common/

Security Monitoring - Base 2.0 Field Sets

The following table lists all the field sets.

Resource	Description	URL
MITRE ATT&CK	This field set selects fields related to MITRE ATT&CK.	/All Field Sets/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Filters

The following table lists all the filters.

Resource	Description	URL
MITRE ATT&CK with Attacker and Target	This filter selects events with MITRE ATT&CK information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	/All Filters/ArcSight Foundation/Common/Shared filters/
Microsoft Windows Security Events	This filter contains the conditions for Microsoft Windows security events.	/All Filters/ArcSight Foundation/Common/Shared filters/Windows/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	/All Filters/ArcSight Foundation/Common/Shared filters/
After Work Hour	The default working hours are from 7 AM to 7 PM.	/All Filters/ArcSight Foundation/Common/Shared filters/
MITRE ATT&CK	This filter selects events with MITRE ATT&CK information.	/All Filters/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Integration Commands

The following table lists all the integration commands.

Resource	Description	URL
----------	-------------	-----

MITRE ATT&CK Lookup	This integration command is used to lookup for the MITRE ATT&CK technique details.	/All Integration Commands/ArcSight Foundation/MITRE ATT&CK/
---------------------	------------------------------------------------------------------------------------	-------------------------------------------------------------

Security Monitoring - Base 2.0 Integration Configurations

The following table lists all the integration configurations.

Resource	Description	URL
MITRE ATT&CK Lookup	This integration configuration is used to configure the MITRE ATT&CK lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Packages

The following table lists all the packages.

Resource	Description	URL
Security Monitoring - Base	This package contains shared resources required by Security Threat Monitoring and Threat intelligence Platform packages.	/All Packages/ArcSight Foundation/

Security Monitoring - Base 2.0 Queries

The following table lists all the queries.

Resource	Description	URL
Mitre Details Summary	This query selects MITRE details summary.	/All Queries/ArcSight Foundation/MITRE ATT&CK/
Mitre by Tactic	This query selects MITRE by tactic.	/All Queries/ArcSight Foundation/MITRE ATT&CK/
Mitre by Id	This query selects MITRE ID.	/All Queries/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Query Viewers

The following table lists all the query viewers.

Resource	Description	URL
MITRE by ID	This query viewer displays MITRE by ID.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/
MITRE by Tactic	This query viewer displays MITRE by tactic.	/All Query Viewers/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Reports

The following table lists all the reports.

Resource	Description	URL
MITRE ATT&CK Summary	This report displays a summary of MITRE ATT&CK events by MITRE ID, Tactics, and Rules.	/All Reports/ArcSight Foundation/MITRE ATT&CK/

Security Monitoring - Base 2.0 Use Cases

The following table lists all the use cases.

Resource	Description	URL
Mitre Att&ck Overview	This use case contains the resources for MITRE ATT&CK.	/All Use Cases/ArcSight Foundation/

Security Monitoring - Base - Active Lists 2.0 Resources By Type

This section lists all Security Monitoring - Base - Active Lists 2.0 Resources by type.

Security Monitoring - Base - Active Lists 2.0 Active Lists

The following table lists all the active lists.

Resource	Description	URL
Application List	This active list contains suspicious applications	/All Active Lists/ArcSight Foundation/Common/
Privilege User Groups	<p>This active list should be populated with the user groups that have administrative privileges in your domain.</p> <p>Entries in this list should be in upper case in the following formats:</p> <ul style="list-style-type: none">• domain\group For example: EMEA\ADMINS• builtin\group For example: BUILTIN\ADMINISTRATORS	/All Active Lists/ArcSight Foundation/Common/
Indicator Types	This list is in synchronization with the Suspicious Indicator Types active list, which is maintained by two lightweight rules.	/All Active Lists/ArcSight Foundation/Common/
Default Accounts	This active list should be populated with the default accounts of each vendor. Entries in this list should be in upper case, if it is not case sensitive.	/All Active Lists/ArcSight Foundation/Common/
Interzone Communications to Restricted Services	This active list contains restricted services.	/All Active Lists/ArcSight Foundation/Common/
Suspicious Indicator Types	This active lists contains indicator types that triggers a particular rule.	/All Active Lists/ArcSight Foundation/Common/
Suspicious Countries	This active list contains suspicious countries. For example, ITAR prohibited countries.	/All Active Lists/ArcSight Foundation/Common/
Cleartext Protocols	This active list contains cleartext protocols.	/All Active Lists/ArcSight Foundation/Common/
Privilege User Account	This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in upper case, if it is not case sensitive.	/All Active Lists/ArcSight Foundation/Common/
Ransomware Notes	This active list contains known ransomware instruction file names.	/All Active Lists/ArcSight Foundation/Common/
MITRE ATT&CK List	This active list contains MITRE ATT&CK information.	/All Active Lists/ArcSight Foundation/MITRE ATT&CK/
Category for Exploit	This active list stores categories for exploit.	/All Active Lists/ArcSight Foundation/Common/
Uncommonly Used Ports	This active list contains the list of uncommonly used ports.	/All Active Lists/ArcSight Foundation/Common/
Commonly Used Ports	This active list contains the list of commonly used ports.	/All Active Lists/ArcSight Foundation/Common/

Security Monitoring - Base - Active Lists 2.0 Packages

The following table lists all the packages.

Resource	Description	URL
Security Monitoring - Base - Active Lists	This package contains pre-defined active lists and rules required by Security Monitoring - Base.	/All Packages/ArcSight Foundation/

Security Monitoring - Base - Active Lists 2.0 Rules

The following table lists all the rules.

--

Resource	Description	URL
Track Rules with MITRE ID	This rule tracks correlation events when the device custom string 6 label is MITRE ID.	/All Rules/Real-time Rules/
Track Rules Triggered	This rule tracks correlation events when the device custom string 6 label is MITRE ID. It tracks the rules under the Threat Intelligence Platform package as well.	/All Rules/Real-time Rules/

Security Threat Monitoring 2.0 Resources By Type

This section lists all Security Threat Monitoring 2.0 Resources by type.

Security Threat Monitoring 2.0 Active Channels

The following table lists all the active channels.

Resource	Description	URL
Entity Monitoring Main Channel	This active channel shows all the entity monitoring category correlation events in the last hour.	/All Active Channels/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Unsuccessful Logins	This active channel shows unsuccessful logins in the last hour.	/All Active Channels/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/

Security Threat Monitoring 2.0 Active Lists

The following table lists all the active lists.

Resource	Description	URL
Suspicious Ransomware Like Activities Tracking	This active list contains ransomware like activities like Shadow Copy Deletion Attempt, Suspicious Access Control List Modifications, and Suspicious Boot Configuration Data Modifications.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Deleted Files On Host	This active list tracks files deleted from the command line on hosts.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Brute Force Attempts	This active list stores information about suspected Brute Force Attempt events. The Brute Force IDS Detected Attempts and Brute Force OS and Application Attempts rules update this active list with attacker system, user account, and target system information.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Malware Target Based Suppression	This suppression list is based on target address and generator name.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
User Account Created	This active list stores the information about the user accounts created within the organization. This active list is updated automatically by a rule and it is used by another rule. By default, the list expires in 24 hours.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Confidential Files	In this active list the customer should fill in the confidential files' names list.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Data Monitoring/
User Accounts Added to Group	This active list stores information about the user accounts added to the groups within the organization. This active list is updated automatically by a rule and it is used by another rule. By default, the list expires in 24 hours.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Exception Email User Domains	The list of exceptional domain should be populated in this active list.	/All Active Lists/ArcSight Foundation/Security Threat Monitoring/Data Monitoring/

Security Threat Monitoring 2.0 Dashboards

The following table lists all the dashboards.

Resource	Description	URL
Unsuccessful Logins from different Countries	This dashboard provides an overview of unsuccessful logins from different countries	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
DNS DGA Monitoring	This dashboard displays DNS DGA statistics.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Malware Activity	This dashboard displays malware statistics.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Members Added and Removed from Privileged Groups	This dashboard provides information about members that are added and removed from the Privileged Group.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Attacks and Suspicious Activity Overview	This dashboard provides an overview of attacks and suspicious activities based on ArcSight Categorization events.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Brute Force Attack Detection	This dashboard displays an overview of suspected Brute Force Attacks.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Vulnerability Overview	This dashboard displays data related to vulnerable assets.	/All Dashboards/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/

Security Threat Monitoring 2.0 Data Monitors

The following table lists all the data monitors.

Resource	Description	URL
Top 10 Attackers	This data monitor displays the top 10 attacker IP addresses.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Top Malicious Domains Accessed	This data monitor displays top DGA domains that are being accessed by the hosts.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Security Indicator - Systems Experiencing High Volume of Failed Logins	This data monitor displays top 10 counts of failed authentication events, grouped by target IP addresses.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Successful Brute Force Login	This data monitor displays the last five successful brute force logins.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Brute Force Attack Attempts	This data monitor displays the last five brute force attack attempts.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Security Indicator - Failed Login Count by User Account	This data monitor displays top 10 counts of failed authentication events, grouped by user account.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Top 10 Attacker Countries	This data monitor displays the top 10 attacker countries.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Latest Attack on Vulnerable Asset	This data monitor displays the latest attacks against vulnerable assets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
Top Addresses Communicating With Malicious Domains	This data monitor displays top addresses that are trying to communicate with malicious domains on the network.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/

Top Vulnerable Asset under Attack	This data monitor displays top assets having vulnerability and are under attack.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
Security Indicator - Most Active Failed Login Source Systems	This data monitor displays top 10 counts of failed authentication events, grouped by attacker IP address.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Members Added and Removed from Privileged Group within 24 Hours	This data monitor displays the last five members that were added and removed from the Privileged Group within 24 Hours.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Attacks and Suspicious Activity per 10 Minutes	This data monitor displays a moving average of attacks. It displays data for the last 10 minutes and generates a correlation event if the moving average is increased by 300%.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Top Malware Names Infections	This data monitor displays top malware names that are infecting the devices.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
All Unsuccessful Logins from different Countries - GeoView	This data monitor shows all the unsuccessful logins from different countries on a map.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Latest Malware Infections on Critical Assets	This data monitor displays last malware infection on High and Very Critical assets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Top Addresses With Malware Infections	This data monitor displays top addresses having malware infections.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Top 10 Targets	This data monitor displays the top 10 attacks and suspicious activity targets.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Unsuccessful Login Count by Country	This data monitor displays top 10 counts of failed authentication events, grouped by source country.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Last 10 Attacks and Suspicious Activity Events	This data monitor displays the last 10 attack and suspicious activity events.	/All Data Monitors/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/

Security Threat Monitoring 2.0 Fields

The following table lists all the fields.

Resource	Description	URL
getCMDLine	This variable returns the field Destination Service Name if the product is Sysmon, else it returns Device Custom String4 as the command line input.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
getParentProcess	This variable returns the field Source Process Name if the product is Sysmon, else it returns File Path as the parent process.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
getTargetProcessName	This variable returns the Target Process Name without the path in lowercase.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
suspiciousTrack_ScheduledTask	This variable returns a string of scheduled tasks.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
suspiciousTrack_JobScheduling	This global variable concatenates strings for job scheduling tasks.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/

suspiciousTrack_ModifyService	This global variable concatenates strings for suspicious modify services.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
getExploitingCategory	This variable returns category for exploit from a list.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
getInterZoneCommunications	This variable returns service information from the interzone communications to restricted services list.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/
getFileNameFromApplicationsList	This variable gets the active list entries based on the file name.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
FileTransfer	This variable is a constant for file transfer category in the application list	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/constants/
getOldFileNameFromApplicationsList	This variable gets the active list entries based on the old file name.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
getTargetProcessNameFromApplicationList	This variable gets the active list entries based on the target process name.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
suspiciousTrack_NewService	This variable returns string of new service.	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
FileArchiver	This variable is constant for the file archiver category in the application list	/All Fields/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/constants/

Security Threat Monitoring 2.0 Field Sets

The following table lists all the field sets.

Resource	Description	URL
Attacks and Suspicious Activity	This field set contains essential fields that are required to investigate attacks and suspicious activities through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Main Channel	This field set contains essential fields that are required to investigate Entity Monitoring rules and correlation events through active channels.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Vulnerable Asset	This field set displays event field information about asset vulnerabilities.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
DNS DGA	This field set contains event fields that are used to investigate DNS DGA events.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Unsuccessful Logins	This field set contains essential fields required to investigate Unsuccessful Logins through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Members Added and Removed from Groups	This field set contains essential fields required to investigate members added and removed from groups through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/

Malware Events	This field set contains event fields used to investigate malware events.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Brute Force Login	This field set contains essential fields that are required to investigate brute force attacks through active channels and data monitors.	/All Field Sets/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/

Security Threat Monitoring 2.0 Filters

The following table lists all the filters.

Resource	Description	URL
A Member was Added and Removed from Privileged Group within 24 Hours	This filter detects when a user was added and removed from a privileged group using Microsoft Windows events in the last 24 hours.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
File Archiver Process in Application List	This filter filters events where the process name is in the file names active list with the category file archiver.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Device Access	This filter tracks events related to the devices that are being accessed.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Windows File Inclusions	This filter captures the most common form of file inclusions to a Windows server during a code injection attack.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Suspicious Boot Configuration Data (BCD) Modifications	This filter detects suspicious boot configuration data modifications.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
SQL Injection Attempts from Other Devices	This filter identifies the SQL Injection attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Malware Detected - Critical Assets	This filter detects correlation events generated from the Malware Detected rule on high and very high critical assets.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Unsuccessful Logins	This filter identifies failed logins by administrative and non-administrative users.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/
Shadow Copy Deletion	This filter identifies shadow copy deletion events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
A Member was Added into a Group	This filter detects when a user is added into a group using Windows events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Login Attempts	This filter detects the attempts to log in to the systems. It excludes machine logins into Microsoft Windows systems.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/
Account Lockouts	This filter identifies account lockouts. By default, it recognizes lockouts on Microsoft Windows and Unix systems.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Windows Events with a Non-Machine User	This filters identifies Microsoft Windows events that have a non-machine/system user either in the attacker or the target fields.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/
Cross Site Scripting from Other Devices	This filter detects Cross Site Scripting attacks from other device vendors.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Successful Brute Force Login	This filter detects correlation events generated by the Successful Brute Force Login rule.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Brute Force/
Unsuccessful Logins with Geo Information	This filter selects failed logins events from different countries with populated Geo fields for both the attacker and target addresses.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Authentication/

DNS DGA	This filter captures events that the Microsoft DNS DGA connector reports as randomly generated domains used by attackers to evade detection.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
All Firewall Deny Traffic	This filter identifies events which indicate denied traffic from firewalls.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/
Removable Device Detected	This filter identifies all removable (storage) devices events by McAfee Data Loss Prevention and Symantec Endpoint Encryption software.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Brute Force Attack Attempts	This filter detects correlation events generated by the following rules: <ul style="list-style-type: none"> • Brute Force OS and Application Attempts • Brute Force IDS Detected Attempts 	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Brute Force/
Suspicious Access Control List Modifications	This filter detects suspicious discretionary access control lists modifications.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Format String Attack Attempts from Other Devices	This filter identifies the format strings attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
HTRAN Detected	This filter contains HTRAN signature detected events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Security Accounts Manager Access Tools	This filter contain the tools that are being used to access the Security Account Manager.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Malware Detected	This filter detects correlation events generated from the Malware Detected rule. Such an event is an alert about host malware infection.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Attack Vulnerable Asset	This filter detects assets that have vulnerabilities.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
Account Deletion	This filter identifies account deletion events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Attacks and Suspicious Activity	This filter identifies events that indicate compromise, reconnaissance, hostile, or suspicious activity.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Directory Traversal Attempts from Other Devices	This filter identifies the Directory Traversal attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Microsoft Windows Events	This filter selects Microsoft Windows events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Service Stopped	This filter identifies the service stop events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Code Injections from Other Devices	This filter identifies the code injection attacks captured from IDS, Antivirus, and other application devices.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
All IDS Events	This filter captures all IDS events based on categorization.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Source and Destination Address not Null	This filter identifies events in which the source and destination address are not null.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Service Failed	This filter identifies the service failed events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
A Member was Removed from a Group	This filter detects when a user is removed from a group using Windows events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Linux File Inclusions	This filter captures the most common form of file inclusions to a Linux server during a code injection attack.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/

File Transfer Process in Application List	This filter filters events where the process name is in the file names active list with the category file transfer.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
All Firewall Accept Traffic	This filter identifies events that indicate accepted traffic from firewalls.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/
File Creation and Modification	This filter identifies the file create events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Windows Events/
Information Transfer to Removable Storage Device	This filter tracks any information transfer to a removable storage device.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Account Creation	This filter identifies account creation events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Accounts/
Process Create	This filter identifies process create events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Windows Events/
Any Process in Application List	This filter filters events where the process name is in the file names active list.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/Process Monitoring/
Web Server Activity Events	This filter captures all Web Server Activity related events.	/All Filters/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/

Security Threat Monitoring 2.0 Packages

The following table lists all the packages.

Resource	Description	URL
Security Threat Monitoring	This package contain default security threat monitoring content.	/All Packages/ArcSight Foundation/

Security Threat Monitoring 2.0 Queries

The following table lists all the queries.

Resource	Description	URL
Top Addresses With Malware Infections	This query pulls the top infected hosts from the Malware Target Based Suppression active list.	/All Queries/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Top Malware Name Infections	This query pulls top malware names that are infecting devices.	/All Queries/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Asset Vulnerability	This query detects assets associated with vulnerabilities.	/All Queries/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
Last 10 Members Added into a Privileged Group	This query displays the last 10 accounts that were added to a privileged group and not removed within 24 hours.	/All Queries/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
All Malware Infections	This query pulls all malware alerts from the Malware Target Based suppression list.	/All Queries/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/

Security Threat Monitoring 2.0 Query Viewers

The following table lists all the query viewers.

Resource	Description	URL
Top Addresses With Malware Infections	This query viewer displays top addresses with malware infections.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/

Members Added into a Privileged Groups	This query viewer displays the last 10 accounts that were added to a privileged group and not removed within 24 hours.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
All Malware Infections	This query viewer displays all malware alerts.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Top Malware Name Infections	This query viewer displays top malware names that are infecting the devices.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Asset Vulnerability	This query displays assets with vulnerabilities.	/All Query Viewers/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/

Security Threat Monitoring 2.0 Rules

The following table lists all the rules.

Resource	Description	URL
New Process Created by InstallUtil	This rule detects when a new process is created by Installutil.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
A Member was Added and Removed from Privileged Group within 24 Hours	This rule detects when a user was added and removed from a privileged group within 24 hours using Windows events.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Multiple Attempts to Discover User Accounts	This rule fires when an attacker tries to discover multiple user accounts present in the local and security groups.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
PowerShell Invoke-command Executed on Remote Host	This rule detects if the PowerShell Invoke-command is executed on a remote host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
Login after Work Hour	This rule triggers when you login after the defined working hours.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Suspicious Access Control List Modifications	This rule adds Suspicious Discretionary Access Control List Modifications events to the Suspicious Ransomware Activities Tracking active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Data Loss through Network Shared Drive	This rule fires whenever a data loss occurs through a network shared drive.	/All Rules/ArcSight Foundation/Security Threat Monitoring/D: Monitoring/
Key Created At Silent Process Exit Registry Folder	This rule triggers when a key is created at: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Data Loss through Email Redirect	This rule triggers when there is a suspected data loss through email redirects.	/All Rules/ArcSight Foundation/Security Threat Monitoring/D: Monitoring/

MSBuild.exe Executed on Non Development Environment	This rule detects if the file MSBuild.exe is executed on a non-development machine.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
User Account Created and Deleted within 24 Hours	This rule identifies an anomalous behavior of user account creation, then deletion within 24 hours (Default TTL: 24 Hours). The rule triggers a correlation event which is sent to a Triage main channel. This rule uses an active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Security Accounts Manager Accessed Through Unauthorized Tools	This rule creates a correlation event when the Security Accounts Manager is accessed through unauthorized tools.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
A Member was Added into a Privileged Group	This rule detects when a user is added into a privileged group using Windows events.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Linux Audited Kernel Module Loaded in Critical Server	This rule triggers by loading the Linux Kernel module. This rule needs special instruction to install the connector and configure logs: https://sec.microfocus.com/foswiki/bin/view/ArcSightActivate/PLinuxOSConnectorInstallation	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Malicious PowerShell Commandlets	This rule detects malicious PowerShell commandlets, which run on your environment.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Data Transfer over Main Channel to C2 Server	This rule creates a correlation event when there is communication between a command and control server over the main channel.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Data Loss through Email	This rule fires when a data loss occurs through outgoing emails.	/All Rules/ArcSight Foundation/Security Threat Monitoring/D Monitoring/
Egress DNS Communications Passed by Firewall	This rule detects egress DNS communications passed by the firewall.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimete Monitoring/
Code Execution Through .lnk File	This rule triggers when a malicious code is executed by the .lnk file.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
User Account Created	This rule fires when a user account is created.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Successful Brute Force Login	This rule detects successful authentication event after suspected brute force attempt. The rule triggers when the user account, attacker system, and target system information of successful authentication event matches an entry in the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/

Files Deleted On A Host	This rule tracks files deleted from a command line interface on a host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Exploit of Client Application	This rule detects the execution of exploit on client applications (like web browsers, Microsoft Office, Adobe Reader, and Flash).	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Dynamic Data Exchange Related Attack	This rule detects attacks leveraging the Dynamic Data Exchange (DDE) technology.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Data Loss through Screen Capture	This rule fires when data loss occurs through screen capture	/All Rules/ArcSight Foundation/Security Threat Monitoring/Data Monitoring/
New Scheduled Task Created	<p>This rule detects when a new scheduled task is created using Windows events.</p> <div> <p>Note</p> <p>Windows Event 602 also covers the changes to the scheduled task.</p> </div>	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/New Scheduled Task Created
New Child Process Launched by CMSTP	This rule detects when a new child process is launched by the file CMSTP.exe.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Data Compression Process Started on Critical Host	This rule creates a correlation event when a process from the applications active list is started on a critical host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Multiple Failed Login to Different Accounts from Single Source	This rule fires when it detects multiple failed logins to different accounts from the same source.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Psexec Tool Execution	This rule detects the execution of sysinternals PsExec tool.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Cleartext Protocol Crossing a Perimeter	This rule detects Cleartext Protocols crossing a Perimeter.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/
External Device With autorun.inf Detected	This rule detects whenever an external drive is plugged with autorun.inf	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Information Transfer to Removable Storage Device	This rule creates a correlation event when information is transferred to a removable external device.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Malicious Control Panel File Detected	This rule triggers when a Malicious Control Panel file is detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/

Execution through Module Load	This rule detects exploit execution through dll.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Execution of Processes with Trailing Spaces	This rule detects execution of Linux processes with trailing spaces.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
HTRAN Signature Detected	HTRAN is a tool that makes proxy connections through intermediate hops and helps users in disguising their true geographical location. It can be used by adversaries to hide their location when interacting with the victim networks.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Data Loss through Clipboard Data	This rule is fired when there is a data loss through the clipboard data.	/All Rules/ArcSight Foundation/Security Threat Monitoring/D: Monitoring/
Suspicious Use of MSXSL.EXE	This rule detects suspicious use of msxsl.exe.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Suspicious Use of WMIC	This rule detects suspicious use of wmic.exe.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Regsvcs or Regasm Making Network Connection	This rule detects network connections initiated by Regsvcs/Regasm.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Detected Cross Site Scripting	This rule detects Cross Site Scripting attacks to the application server through the request URLs and also from other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Consecutive Unsuccessful Logins to Same Account from different IPs	This rule triggers when it detects a set of three consecutive unsuccessful logins to the same account from three different IP addresses.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
High Severity IDS Event	This rule detects all the high severity exploit attacks simulated through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
CMSTP Involved on Network Connection	This rule detects network connections initiated by CMSTP.exe	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
MetaSploit Detected	This rule detects if the Metasploit framework is installed on the system using assessment tools.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H: Monitoring/

Consecutive Unsuccessful Logins to Same Account from different Countries	This rule triggers when it detects a set of three consecutive unsuccessful logins to the same account from three different countries.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
VNC Exploit Execution	This rule detects the execution of potential exploit on VNC related software.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Track Modified Service	This rule tracks modified services.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Attack To Vulnerable Asset	This rule triggers when it detects an exploitation attempt on a vulnerable asset.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Vulnerab Monitoring/
Credential Dumping through Keefarce	This rule triggers when Credential Dumping is practiced through Keepfarce.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Multiple Unique IDS Events to Same Destination	This rule detects multiple unique IDS events that gather information from IDS. This rule gets triggered only where there are four unique IDS events in a span of 30 minutes to the same destination.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Script Executed On Critical Host	This rule triggers when a script is executed on a critical host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Pass The Hash	This rule detects Pass The Hash attack attempts on Windows machines. On each detection, the rule adds target addresses in the suppression list to avoid multiple alerts on the same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
HTA File Download	This rule detects a host that is trying to download a .HTA file.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Multiple Services Down on Same Host	This rule detects multiple services going down on same host in a 30 minutes time lapse. On each detection, the rule adds target address in the suppression list to avoid multiple alerts on same address in a short period of time. By default, this rule is disabled due to possible performance impact.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Authentication Attempted to Disabled Account	This rule detects authentication attempted to a disabled account.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Large Information Transfer to Removable Storage Device	This rule creates a correlation event when a large file transfer to a removable storage device is detected.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Suspicious Activity after New Service	This rule triggers when suspicious activities occur after adding a new service.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/

MSXSL.exe Detected on Non Development Environment	This rule detects DLL Hijacking activity by PowerSploit.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Detected DLL Hijacking Activity by PowerSploit	This rule detects DLL Hijacking activity by PowerSploit.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Suspicious Activity after Modify Service	This rule triggers when suspicious activities occur after adding a new service.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Suspicious Powershell Command Line Argument Detected	This rule detects suspicious PowerShell command line arguments.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Logging Service On Host Has Stopped	This rule triggers when the logging service on the host has stopped.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Host Firewall Has Stopped	This rule triggers when the host firewall service has stopped on the host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Removable Device Blocked On Host	This rule triggers when a removable device is blocked on a host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
DLL File Has been Modified On Critical Host	This rule triggers when a DLL file is modified on a critical host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Detected Format String Attack	This rule detects format string attacks.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Shell Command Execution	This rule detects the execution of potential Shell commands and Shell code attacks.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Privileged Account Locked Out	This rule detects account lockouts.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
PowerShell Executed From Browser	This rule detects the execution of PowerShell from a browser.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
High Volume of Denies to Same Destination	This rule detects a high volume of denies to the same destination.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimete Monitoring/

Image File Execution Options Injection	This rule detects Image File Execution Options Injection using the reg.exe command.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Data Transfer over Alternative Protocol to C2 Server	This rule creates a correlation event when there is communication between a command and control server over alternative protocol.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Detected Squiblydoo Attack	This rule detects Squiblydoo attack.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
InstallUtil Involved on Network Connection	This rule detects network connections initiated by InstallUtil.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Detected Enabled DCOM	This rule detects whether DCOM is enabled on the system using vulnerability scanner events.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Base64 File Has Been Decoded On Host	This rule triggers when a base64 file is decoded on a host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Malware Detected	This rule detects malware activities on the devices. On each detection, the rule adds target addresses in the suppression list to avoid multiple alerts on the same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Detected Code Injection	This rule detects code injection attacks to the application server that occur through the request URLs, and also from other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
External Device On Machine Infected With Malware	This rule triggers if there is a malware infection on a machine where an external drive was plugged with autorun.inf.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
JavaScript Code Executed through rundll32	This rule detects JavaScript Code executed through rundll32.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Exploit Attempt Detected by IDS	This rule detects exploit attacks through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Suspicious Boot Configuration Data Modifications	This rule adds suspicious Boot Configuration Data modifications events to the Suspicious Ransomware Activities Tracker active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/

Possible Ransomware Detected	<p>This rule triggers when one of the following conditions are met:</p> <ul style="list-style-type: none"> • Large file modifications in the user directory (shadow copy deletion attempt or suspicious access list modifications or suspicious boot configuration data modifications) • Two different events from shadow copy deletion attempt, suspicious access list modifications, suspicious boot configuration data modifications. 	/All Rules/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Default Account Enabled	This rule triggers when a default account is enabled.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
File Deleted On Malware Infected host	This rule triggers when files are deleted on a malware infected host.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Suspicious Activity after Scheduled Task	This rule triggers when suspicious activities occur after scheduled task is created or updated.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Detected SQL Injection	This rule detects SQL Injection attacks to the application server through the request URLs, and also from other IDS and application devices.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
Abnormal Use of hh.exe	This rule detects abnormal use of the hh.exe command.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
Privilege Escalation Attempt Detected	This rule detects privileged exploit attacks through various ways of gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Suspicious Activity after Local Job Changes	This rule triggers when suspicious activities occur after local scheduled job is changed.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Brute Force IDS Detected Attempts	This rule detects brute force attack attempts detected by IDS. The rule triggers when ArcSight ESM receives a brute force attack attempt event from IDS. On the first event, the user account, attacker system, and target system information is added to the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Shadow Copy Deletion Attempt	This rule adds events with process command line parameters that contain commands to delete the shadow copies in the Suspicious Ransomware Activities Tracker active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Track Job Scheduling Change	This rule triggers when changes are made to the file /etc/crontab.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Audit Cleared Log	This rule detects an audit log cleared event. On each detection, the rule adds target addresses in the suppression list to avoid multiple alerts on the same address in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/

API Hooking Detected	This rule detects API Hooking using the volatility apihooks plugin.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Multiple Access Attempts To Malicious Domains From Same Source Address	This rule detects multiple access attempts on malicious domains from the same source address.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Powershell Script Executed by SyncAppvPublishingServer	This rule detects if the PowerShell script is executed by SyncAppvPublishingServer.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Detected DLL Injection by Mavinject.exe	This rule detects dll injection by Mavinject.exe.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Detected Directory Traversal	This rule triggers when it detects the directory traversal attacks.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Consecutive Unsuccessful Logins to Administrative Account	This rule detects a set of five consecutive unsuccessful logins to the privilege account within one minute.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Suspicious Use of Msiexec.exe	This rule detects suspicious use of Msiexec.exe.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Windows Remote Management Enabled by PowerShell	This rule detects whether Windows Remote Management is enabled using PowerShell.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Egress Restricted Services Communications Passed by Firewall	This rule detects egress communications to restricted services passed by the firewall.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimete Monitoring/
Track Scheduled Task	This rule tracks scheduled tasks and writes them down on the Suspicious Activities Tacking active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/
Multiple RDP Connections from the Same Host in Short Period of Time	This rule detects multiple RDP connections from the same host in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicati Monitoring/
Suspicious Data Transfer Process Started From Command Line	This rule creates a correlation event when a process from the Applications active list is started from the command line.	/All Rules/ArcSight Foundation/Security Threat Monitoring/H Monitoring/

Information Transfer to Removable Device	This rule creates a correlation event when information is transferred to a removable external device.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Egress Communications to Suspicious Country	This rule detects Egress communications to a suspicious country.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Perimete Monitoring/
Log into Multiple Systems in Short Period	This rule triggers when you log in to multiple systems in a short time period.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Registry Injection	This rule detects any modification on Appinit_DLL, AppCertDlls and IFEO (Image File Execution Options) which are registry keys that malware usually modifies for injection and persistence.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Mshta Command Execution	This rule detects Mshta command executions.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
Track New Service	This rule tracks new services.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Key Created At Image File Execution Options Registry Folder	This rule triggers when a key is created at: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Option	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/
Brute Force OS and Application Attempts	This rule detects brute force attacks on OS and applications. The rule triggers when the failed authentication event from the same attacker system using the same user account to the same target system exceeds the threshold. On the first threshold, information about user account, attacker system, and target system is added to the Brute Force Attempts active list.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Suspicious Use of PubPrn.vbs	This rule detects suspicious use of PubPrn.vbs.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
DoS Activity Detected by IDS	This rule detects Network Denial of Service attacks by gathering information from IDS.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Multiple RDP Connections from the Same User in Short Period of Time	This rule detects multiple RDP connections from the same user in a short period of time.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Applicatio Monitoring/
Large amount of file modifications in users directories	This rule triggers when there is a large amount of file creation/modification in user directories.	/All Rules/ArcSight Foundation/Security Threat Monitoring/Ht Monitoring/

Security Threat Monitoring 2.0 Use Cases

The following table lists all the use cases.

Resource	Description	URL
Network Monitoring	This use case contains resources for network monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/
Malware Monitoring	This use case contains resources for malware monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Malware Monitoring/
Security Threat Monitoring	This is a master use cases, and it contains multiple child use cases.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/
Account Activity	This use case includes different resources to monitor the account activities given below: <ul style="list-style-type: none"> • Authentication Attempts to Disabled Account. • Privileged Account Locked Out • Members added and removed from privileged groups within 24 hours • User Accounts created and deleted within 24 hours 	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Unsuccessful User Logins	This use case includes different resources to monitor the unsuccessful login activities given below: <ul style="list-style-type: none"> • Consecutive Unsuccessful Logins to Administrative Account • Consecutive Unsuccessful Logins to Same Account from different Countries • Consecutive Unsuccessful Logins to Same Account from different IPs • Multiple Failed Login to Different Accounts from Single Source • General Unsuccessful Logins • Failed Login count by user accounts, source, and destination systems 	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Brute Force Attacks	This use case tracks brute force login attempts and generates alerts for successful brute force attacks.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/
Vulnerability Monitoring	This use case contains resources that are included in vulnerability monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Vulnerability Monitoring/
Host Monitoring	This use case contains resources that are included in host monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Host Monitoring/
Perimeter Monitoring	This use case is focused on events related to boundary transitions and connections between entities.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Perimeter Monitoring/
Application Monitoring	This use case contains resources for application monitoring.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Application Monitoring/
Attacks and Suspicious Activity Overview	This use case includes different resources to monitor attacks and suspicious activities reported by ArcSight Connectors based on ArcSight Categorization.	/All Use Cases/ArcSight Foundation/Security Threat Monitoring/Network Monitoring/

Threat Intelligence Platform 2.0 Resources By Type

This section lists all Threat Intelligence Platform 2.0 Resources by type.

Threat Intelligence Platform 2.0 Active Lists

The following table lists all the active lists.

Resource	Description	URL
Exception Addresses	This active list enables you to define IP addresses that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/

Suspicious Addresses List	This active list contains suspicious addresses collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious Domain	This active list enables you to define a suspicious domain.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Suspicious URL List	This active list contains suspicious URLs collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Email List	This active list contains suspicious email addresses collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception URL	This active list enables you to define URLs that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Additional Suspicious Email	This active list enables you to define a suspicious email.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Internal Domain Found in Suspicious Domains List	This active list stores internal domains that are found in the suspicious domain list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception Hash	This active list enables you to define a hash that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Suspicious Domain List	This active list contains suspicious domains collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Internal Address Found in Reputation Data	This active list stores internal IP addresses that are found in the reputation list.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Additional Suspicious URL	This active list enables you to define suspicious URL.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Additional Suspicious Hash	This active list enables you to define a suspicious hash.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Exception Email	This active list enables you to define an email that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Additional Suspicious Addresses	This active list enables you to define suspicious IP addresses.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/
Suspicious Hash List	This active list contains suspicious hash collected from MISP Circl.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/
Exception Domain	This active list enables you to define a domain that will not be considered suspicious.	/All Active Lists/ArcSight Foundation/Threat Intelligence Platform/User Defined Reputation Data/

Threat Intelligence Platform 2.0 Dashboards

The following table lists all the dashboards.

Resource	Description	URL
Threat Intelligence Overview	This dashboard displays overview of threat intelligence alerts.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/
Reputation Data Overview	This dashboard displays reputation data overview.	/All Dashboards/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform 2.0 Fields

The following table lists all the fields.

Resource	Description	URL
dstAdditionalDomainLevel4	This variable retrieves threat metadata defined by the user from the Additional Suspicious Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/

srcAddressIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstExceptionDomainLevel2	This variable retrieves exception domain from the Exceptions Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
hashIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
srcAdditionalEmailEntry	This variable returns the entry of a source in the Additional Suspicious Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
dstDomainIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
hashIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
getSrcDomainList	This variable returns the source domain in list format separated by a dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
dstDomainIndicatorType	This global variable displays the domain indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getSizeOfDstDomainList	This variable returns the size of the destination domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
hashIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
dstAddressIndicatorType	This variable returns an indicator type for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
srcAddressIndicatorTypeList	This variable returns a list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
exceptionFileHashEntry	This variable retrieves the threat metadata from the Exception Hash based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
srcExceptionDomainLevel4	This variable retrieves the exception domain from the Exceptions - Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcSuspiciousListDomainLevel3	This variable retrieves threat metadata from the Suspicious Domain List active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstAddressIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
getDstDomainList	This variable returns the destination domain in list format separated by a dot.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
srcSuspiciousListDomainLevel4	This variable retrieve threat metadata from the Suspicious Domain List active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/

srcSuspiciousEmailEntry	This variable returns the entry of a source in the Suspicious Email active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
srcSuspiciousDomainEntry	This variable retrieves the threat metadata from the Suspicious Domain List based on a source that has a fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstAddressReference	This variable returns reference for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstAdditionalDomainLevel2	This variable retrieves threat metadata defined by the user from the Additional Suspicious Domain active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
suspiciousFileHashEntry	This variable retrieves the threat metadata from the Suspicious Hash List active list based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
hashIndicatorTypeList	This variable returns a list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
getDstDomainLevel2	This variable returns the two rightmost destination sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
srcEmailIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
getRequestURLDomain	This variable returns the domain from the request URL.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
getSrcDomainLevel1	This variable returns the rightmost source sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
srcDomainIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getSizeOfSrcDomainList	This variable returns the size of the source domain list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
srcAdditionalDomainLevel4	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstDomainReference	This variable returns reference for the destination domain either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstExceptionAddressEntry	This variable retrieves the threat metadata from the Exception Addresses List active list based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
getDstDomainLevel4	This variable returns the four rightmost destination sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
additionalFileHashEntry	This variable retrieves the threat metadata from the Additional Suspicious Hash active list based on a filehash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
dstSuspiciousAddressEntry	This variable retrieves the threat metadata from the Suspicious Addresses List active list based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/

dstAddressIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstExceptionDomainLevel3	This variable retrieves the exception domain from the Exceptions Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcSuspiciousListDomainLevel2	This variable retrieves the threat metadata from the Suspicious Domain List active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstAdditionalAddressEntry	This variable retrieves the threat metadata from the Additional Suspicious Addresses List active list based on a destination address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
getSrcDomainLevel3	This variable returns the three rightmost source sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
getDstDomainLevel1	This variable returns the rightmost destination sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
srcAddressIndicatorType	This variable returns an indicator type for the Source address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstDomainIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstExceptionDomainLevel4	This variable retrieves exception domain from the Exceptions Domain active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcAddressIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstSuspiciousListDomainLevel4	This variable retrieves threat metadata from the Suspicious Domain List active list corresponding to the destination domain level 4.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcDomainIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getDstDomainLevel3	This variable returns the three rightmost destination sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Destination/
srcAdditionalAddressEntry	This variable retrieves the threat metadata from the Additional Suspicious Addresses List active list based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
srcEmailIndicatorType	This global variable displays the email indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
srcDomainIndicatorTypeList	This variable returns a list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getSrcDomainLevel2	This variable returns the two rightmost source sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
srcDomainIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/

dstAddressValue	This variable returns addresses for the destination address either from the Suspicious Addresses List active list or the Additional Suspicious Addresses active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
srcDomainIndicatorType	This global variable displays the domain indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstDomainValue	This variable returns domains for the destination domains either from the Suspicious Domain List active list or the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcExceptionDomainLevel3	This variable retrieves the exception domain from Exceptions - Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcAdditionalDomainEntry	This variable returns the entry of a source in the Additional Suspicious Domain active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstDomainIndicatorType2	This variable returns the second indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getSrcDomainLevel4	This variable returns the four rightmost source sub-domains that follow the dotted format.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/By Source/
srcEmailIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
dstAdditionalDomainEntry	This variable retrieves the threat metadata from the Additional Suspicious Domain List active list based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcEmailIndicatorTypeList	This variable returns a list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
dstAddressIndicatorType3	This variable returns the third indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
srcAdditionalDomainLevel3	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcExceptionAddressEntry	This variable retrieves the threat metadata from the Exception Addresses List active list based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
srcExceptionDomainLevel2	This variable retrieves exception domain from the Exceptions - Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
getHashValue	This variable retrieves the hash value from fields - File Hash and Old File Hash.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
srcAdditionalDomainLevel2	This variable retrieves additional domain from the Additional Suspicious Domain active list corresponding to the source domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcEmailValue	This variable returns emails either from the Suspicious Email List active list or the Additional Suspicious Emails active list.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
srcEmailIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/

srcSuspiciousAddressEntry	This variable retrieves the threat metadata from the Suspicious Addresses List active list based on a source address.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstAdditionalDomainLevel3	This variable retrieves the threat metadata defined by the user from the Additional Suspicious Domain active list corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcExceptionDomainEntry	This variable retrieves the exception domain from the Exceptions - Domain active list based on a source fully that has a qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
hashIndicatorType	This global variable displays the hash indicator types.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Hash/
dstSuspiciousListDomainLevel3	This variable retrieves the threat metadata from the Suspicious Domain List active corresponding to the destination domain level 3.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
srcAddressIndicatorType1	This variable returns the first indicator type.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/
dstSuspiciousDomainEntry	This variable retrieves the threat metadata from the Suspicious Domain List active list based on a destination that has a fully qualified domain name or hostname.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstSuspiciousListDomainLevel2	This variable retrieves the threat metadata from the Suspicious Domain List active list corresponding to the destination domain level 2.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstDomainIndicatorTypeList	This variable returns a list of indicator types separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstExceptionDomainEntry	This variable retrieves the threat metadata from the Exception Domain List active list based on a destination domain.	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Domain/
dstAddressIndicatorTypeList	This variable returns list of indicator type separated by .	/All Fields/ArcSight Foundation/Threat Intelligence Platform/Suspicious Address/

Threat Intelligence Platform 2.0 Filters

The following table lists all the filters.

Resource	Description	URL
Destination in Suspicious Domain List	This filter identifies the destination domain in the Suspicious Domain List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Destination in Suspicious Domain	This filter detects all events which destination is in the suspicious or additional domain list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
C2 Inbound Communication from a Suspicious Domain	This filter contains correlated events of Command and Control Inbound communication from a suspicious domain.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Source in Suspicious Domain List	This filter identifies the source domain in the Suspicious Domain List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Destination in Suspicious Address List	This filter identifies the destination address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/

C2 Inbound Communication from a Suspicious Address	This filter contains correlated events of Command and Control Inbound communication from a suspicious address.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Source in Suspicious Email List	This filter identifies the source email address in the Suspicious Email List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/
Source in Suspicious Address List	This filter identifies the source address in the Suspicious Addresses List active list.	/All Filters/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform 2.0 Integration Commands

The following table lists all the integration commands.

Resource	Description	URL
VirusTotal Hash Lookup	This integration command is used to lookup for hash details using VirusTotal.	/All Integration Commands/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform 2.0 Integration Configurations

The following table lists all the integration configurations.

Resource	Description	URL
VirusTotal Hash Lookup	This integration configuration is used to configure the VirusTotal Hash Lookup command. You can run the command on any cell selected in the viewer.	/All Integration Configurations/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform 2.0 Packages

The following table lists all the packages.

Resource	Description	URL
Threat Intelligence Platform	This package contains default content for threat intelligence platform.	/All Packages/ArcSight Foundation/

Threat Intelligence Platform 2.0 Queries

The following table lists all the queries.

Resource	Description	URL
Threat Intelligence Alerts Details	This query selects the alert details triggered by the threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Hash by Indicator Type	This query selects indicator type and counts from the suspicious hash list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Domain by Indicator Type	This query selects indicator type and counts from the suspicious domain list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Top Alerts by Attacker	This query selects attacker addresses triggered by the threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Top Alerts by Target	This query selects target addresses triggered by the threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Threat Intelligence Alerts by Type	This query selects the rule group name triggered by the threat intelligence platform rules.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
Suspicious Address by Indicator Type	This query selects indicator type and counts from the suspicious address list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/

Suspicious URL by Indicator Type	This query selects indicator type and counts from the suspicious URL list.	/All Queries/ArcSight Foundation/Threat Intelligence Platform/
----------------------------------	----------------------------------------------------------------------------	----------------------------------------------------------------

Threat Intelligence Platform 2.0 Query Viewers

The following table lists all the query viewers.

Resource	Description	URL
Top Indicator Type in Suspicious Hash	This query viewer displays top indicator types in the suspicious hash list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious URL	This query viewer displays top indicator types in the suspicious URL list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious Domain	This query viewer displays top indicator types in the suspicious domain list.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Last 20 Threat Intelligence Alerts	This query viewer displays last 20 threat intelligence alerts.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Threat Intelligence Alerts by Attacker	This query viewer displays top alerts by attacker address.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Threat Intelligence Alerts by Type	This query viewer displays threat intelligence alerts by type.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Threat Intelligence Alerts by Target	This query viewer displays top alerts by target address.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Threat Intelligence Alerts Details	This query viewer displays threat intelligence alerts details.	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/
Top Indicator Type in Suspicious Address	This query viewer displays top indicator types in suspicious address list	/All Query Viewers/ArcSight Foundation/Threat Intelligence Platform/

Threat Intelligence Platform 2.0 Rules

The following table lists all the rules.

Resource	Description	URL
Outbound Communication to a Phishing Address	This rule triggers when there is outbound traffic to a suspicious phishing site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Phishing/
Outbound Communication to a Phishing Domain	This rule triggers when there is outbound traffic to a suspicious phishing domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Phishing/
Received Email From Phishing Address	This rule triggers when an email is received from a phishing address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Received Email From Malware Address	This rule triggers when an email is received from a malware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Email Sent To Suspicious Address	This rule triggers when an email is sent to a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Malware Activity to a Suspicious Domain	This rule triggers when there is outbound traffic to a suspicious malware site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/
Command and Control Outbound Communication on Uncommonly Used Port	Adversaries may conduct Outbound C2 communications over a non-standard port to bypass proxies and firewalls that have been improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
DNS Query to a Suspicious Address	This rule triggers when there is an outbound suspicious DNS query.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious DNS Query/
Received Phishing Email With An Attachment	This rule triggers when an email containing an attachment is received from a suspicious source.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/

Add Indicator Types	This rule adds indicator type to a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Remove Indicator Types	This rule removes indicator type from a list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Outbound Traffic to a Suspicious Domain	This rule triggers when there is outbound traffic to a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Command and Control Outbound Communication on Commonly Used Port	Adversaries may conduct Outbound C2 communications over a commonly used port to bypass proxies and firewalls that are improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Inbound Traffic from a Suspicious Domain	This rule triggers when there is inbound traffic from a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Command and Control Communication Over Web Services	This rule triggers when adversaries use an existing and legitimate external Web service as a means for relaying commands to a compromised system.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Internal Destination Address Found in Suspicious Address List	This rule triggers when an internal destination address is found in the suspicious address list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/
Command and Control Inbound Communication on Uncommonly Used Port	Adversaries may conduct Inbound C2 communications over a non-standard port to bypass proxies and firewalls that are improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Inbound Traffic from a Suspicious Address	This rule triggers when there is inbound traffic from a suspicious site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Internal Source Domain Found in Suspicious Domain List	This rule triggers when the internal source domain is found in the suspicious domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/
Internal Source Address Found in Suspicious Address List	This rule triggers when the internal source address is found in the suspicious address list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/
Command and Control Communication to a Suspicious Domain	This rule triggers when there is outbound traffic to a suspicious command and control domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Outbound Traffic to a Suspicious Address	This rule triggers when there is outbound traffic to a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Activity/
Command and Control Inbound Communication on Commonly Used Port	Adversaries may conduct Inbound C2 communications over commonly used port to bypass proxies and firewalls that are improperly configured.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Command and Control Communication to a Suspicious Address	This rule triggers when there is outbound traffic to a suspicious command and control server.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/
Malware Activity to a Suspicious Address	This rule triggers when there is outbound traffic to a suspicious malware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Malware/
Dangerous Browsing to a Suspicious Domain	This rule triggers when there is outbound traffic to a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/
Suspicious File Hash Activity in Host	This rule triggers when there is a suspicious file hash in host.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious File Hash/
Received Email From A Command And Control Address	This rule triggers when an email is received from a command and control address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Potential Information Transfer Through Removable Media Over C2 Communication	This rule triggers when potential Information is transferred to a removable media over the command and control server.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Botnet Activity/

Received Email From Ransomware Address	This rule triggers when an email is received from a ransomware address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Internal Destination Domain Found in Suspicious Domain List	This rule triggers when internal destination domain is found in the suspicious domain list.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Internal Asset Found in Reputation List/
Ransomware Activity to a Suspicious Address	This rule triggers when there is outbound traffic to a suspicious ransomware site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Ransomware/
Email Received From Suspicious Address	This rule triggers when an email is received from a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious Email/
Dangerous Browsing to a Suspicious URL	This rule triggers when there is outbound traffic to a suspicious URL.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/
Ransomware Activity to a Suspicious Domain	This rule triggers when there is outbound traffic to a suspicious ransomware site.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Ransomware/
Dangerous Browsing to a Suspicious Address	This rule triggers when there is outbound traffic to a suspicious address.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Dangerous Browsing/
DNS Query to a Suspicious Domain	This rule triggers when there is a DNS query to a suspicious domain.	/All Rules/ArcSight Foundation/Threat Intelligence Platform/Suspicious DNS Query/

Threat Intelligence Platform 2.0 Use Cases

The following table lists all the use cases.

Resource	Description	URL
Threat Intelligence Platform	This use case detects threat based on the intelligence data collected from MISP.	/All Use Cases/ArcSight Foundation/Threat Intelligence Platform/

Send Documentation Feedback

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

Feedback on ArcSight Administration and ArcSight System Standard Content Resources (ESM 7.2 Service Pack 1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!