



ArcSight Recon 1.2

User Guide

May 2021

Copyright Notice

© Copyright 2021 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.

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/about/legal/>.

Contents

About This Book	9
1 Welcome to ArcSight Recon	11
Part I Investigating Events	13
2 Searching for Events	15
Understanding the Search Feature	15
Creating and Saving Searches	16
Create a Search	16
Save a Search	17
Name a Search	17
Find a Saved Search	17
Searching Data Stored by ArcSight Logger	18
Best Practice Considerations for Searching Logger Data	18
Include Logger Data in a Search	18
Initiating a Search from Enterprise Security Manager	18
Understanding the Search Progress Indicators	19
3 Managing Your Searches	21
Viewing Search Results	21
View the Events Timeline	21
View the Events Table	21
View and Use the Details of an Event	23
Identify Fields without Data	23
Refresh Search Results	23
Build a Report Using Search Results	24
Modifying the Search Settings	24
Exporting the Search Results	24
Scheduling Regular Runs of a Search	24
Create a Scheduled Search	25
View Scheduled Searches	26
Clone a Scheduled Search	27
Edit a Scheduled Search	27
Delete a Scheduled Search	27
Enable and Disable a Scheduled Search	27
Managing Completed Runs of a Scheduled Search	28
View a Completed Run of a Scheduled Search	28
Delete Completed Runs of a Scheduled Search	29
Export Completed Runs of a Scheduled Search	29
4 Understanding the Search Parameters	31
Understand the Types of Search Queries	31

Using GlobalEventID in a Query	33
Understand the Query Syntax, Operators, and Functions	33
Understand the Query Syntax Requirements	33
Understand the Search Query Functions and Operators	36
Understand the Functions for Building Eval Expressions	37
Specify a Group of Fields	43
Specify an Alias for a Field	44
Specify IP Addresses and Subnets	47
How Search Stores IP and MAC Addresses	48
Enter an IP or MAC Address	48
Include a Storage Group's Filter in the Search Query	49
Extend the Search with a Lookup List	49
Considerations for the Lookup List File	49
Create a Lookup List	50
Replace a Lookup List	51
Delete a Lookup List	51
Use Specific Sets of Fields for Search Results	51
View and Create Fieldsets	52
Create a Fieldset	52
Edit a Fieldset	53
Delete a Fieldset	53
Clone a Fieldset	54
Configure the Time Range	54
Specify a Dynamic Date Range	54
Base the Search on the Timestamp for Events	55
Understand How Time Zones Affect Search Results	56
Configure Preferred Settings for Searches	56
 Part II Hunting for Undetected Threats	 57
 5 Viewing Dashboards and Reports	 59
View a Dashboard	59
View a Report	60
Choose Default Dashboards for the Reports Portal	60
 6 Understanding the MITRE ATT&CK Dashboards and Reports	 63
MITRE ATT&CK Dashboards	63
MITRE ATT&CK Overview	64
Evaluation Techniques and Tactics Summary	64
MITRE ATT&CK Reports	65
MITRE ATT&CK Destination Address Summary	65
MITRE ATT&CK Destination Host Summary	65
MITRE ATT&CK Destination Username Summary	66
MITRE ATT&CK Source Address Summary	66
MITRE ATT&CK Source Hostname Summary	66
MITRE ATT&CK Source Username Summary	66
MITRE ATT&CK Technique Summary	67
 7 Understanding the Cloud Security Dashboards and Reports	 69
Abuse and Nefarious Use of Cloud Services – Dashboards	70

Account Hijacking – Dashboards and Reports	71
Advanced Persistent Threats – Dashboard	72
Data Breaches – Dashboards	72
Data Loss – Dashboard and Reports	73
Denial of Service – Dashboard	73
Insecure Interfaces and APIs – Report	73
Insufficient Due Diligence – Reports	73
Insufficient Identity Credential and Access Management – Reports	74
Malicious Insiders – Report	74
System Vulnerabilities – Dashboard and Reports	74
Vulnerabilities on Shared Technologies	76
8 Understanding the Foundation Dashboards and Reports	77
Entity Monitoring – Dashboards and Reports	78
Events Overview – Dashboards	79
Hosts Monitoring - Reports	79
Malware Monitoring – Dashboard and Reports	80
Network Monitoring – Dashboards and Report	80
Perimeter Monitoring – Dashboards and Reports	82
Vulnerability Monitoring – Dashboard and Reports	82
9 Understanding the OWASP Security Dashboards and Reports	85
Broken Access Control	86
Broken Authentication	86
Cross-site Scripting	86
Injects	87
Insecure Deserialization – Dashboards and Reports	87
Insufficient Logging and Monitoring – Dashboards and Reports	88
Security Misconfiguration	89
Sensitive Data Exposure	89
Using Components with Known Vulnerabilities – Dashboards and Reports	90
XML External Entities	90
Part III Analyzing Anomalous Data with Outlier Analytics	93
10 Generating Models to View Anomalous Data	95
Considerations for Generating Models	95
Defining and Building a Model	96
Scoring a Model	96
Deleting a Model	97
11 Viewing Anomalous Data in a Model	99
Understand the Provided Analytics Charts	99
Further Investigate Anomalies	100
View a Scored Model	100

Part IV Managing the Quality of Your Data	101
12 Understanding the Data Quality Insights	103
13 Understanding How Data Quality is Calculated	105
14 Analyzing Data Quality	107
Part V Ensuring Data Compliance	109
15 Ensuring Compliance with GDPR Standards	111
Access Activity	114
Access Activity	114
Regulatory Exposure	116
Threat User Analysis	116
Admin Activity	117
Attack Surface Analysis	117
Attack Surface Identification	118
Security Controls Risk Identification	120
Corporate Governance	120
Regulatory Exposure	121
Threat Analysis	123
Data Store Risk	123
Internet Threat Analysis	125
16 Ensuring Compliance with ISO-27002	127
12 – Operations Security	127
17 Ensuring Compliance with PCI DSS	131
Firewall Configuration – Requirement 1	132
Default Security Parameters – Requirement 2	133
Encryption Transmission – Requirement 4	135
Track and Monitor Data Access – Requirement 10	135

Part VI Using Visuals and Reports to Analyze Data	137
18 Accessing Reports and Dashboards	139
19 Scheduling Report Generation	141
20 Designing Dashboards for Data Analysis	143
21 Designing Reports for Data Analysis	145
22 Adding and Removing Report Content	147
Import and Export Content	147
Supported Data Sources	147
23 Best Practices for the Report Designer and Dashboard Designer	149
Using Search Results to Create a Dashboard or Report	149
Build a Report Using Search Results	149
Build a Dashboard Using Search Results	150
Convert the Search Fields to Human-Readable Values	150
Using Data Models to Build a Worksheet	151
Using Data Worksheets to Build a Dashboard or Report	151
Creating a Simple Dashboard	152
Use the Dashboard Wizard	152
Use the Dashboard Editor	152
Creating a Simple Scheduled Report	153
Creating a Simple Report	154
Use the Crosstab Wizard	154
Use the Table Wizard	154
Use the Chart Wizard	155
Guidelines for Report Usage	155
Part VII Managing Your Stored Data	157
24 Organizing Your Data	159
Use Storage Groups to Organize and Retain Data	159
Create a Storage Group	159
Direct Events to the Correct Storage Group	160
Activate and Deactivate Storage Groups	160
Change the Settings of a Storage Group	161
Modify a Storage Group	161
Apply Your Changes to a Storage Group	161
Set Retention Policies for the Data	162
Delete Old Data	162
Use Storage Group Queries in a Search	162

Part VIII Managing User Access and Preferences	163
25 Assigning Permissions for Recon	165
26 Default Roles for Recon	167
27 Configuring User Preferences	169
Configure Search Preferences	169
Part IX Appendices	171
A Mapping Database Names to their Appropriate Search Fields	173
Agent Fields	173
Category Fields	174
Correlation Fields	174
Destination Fields	175
Device Fields	176
Device Custom Fields	177
Event Fields	178
Extension Fields	179
File Fields	179
Flex Fields	179
OldField Fields	180
Old File Fields	180
Request Fields	180
Source Fields	181

About This Book

This *User's Guide* provides concepts, use cases, and contextual help for ArcSight Recon.

- ♦ [Investigating Events](#)
- ♦ [Hunting for Undetected Threats](#)
- ♦ [Analyzing Anomalous Data with Outlier Analytics](#)
- ♦ [Managing the Quality of Your Data](#)
- ♦ [Ensuring Data Compliance](#)
- ♦ [Using Visuals and Reports to Analyze Data](#)
- ♦ [Managing Your Stored Data](#)
- ♦ [Managing User Access](#)

Intended Audience

This book provides information for individuals who investigate events and hunt for undetected threats. These individuals have experience in security operation centers or performing duties of a security analyst or operator.

Additional Documentation

The Recon documentation library includes the following resources:

- ♦ [Release Notes for ArcSight Containerized Platform](#), which provides an overview of the products deployed in the containerized environment and their latest features or updates
- ♦ [Release Notes for ArcSight Recon](#), which provides information about updates or new features available in the current release
- ♦ [Administrator's Guide to ArcSight Platform](#), which provides information about deploying, configuring, and maintaining the products that you deploy in the containerized environment
- ♦ [Technical Requirements for ArcSight Platform](#), which provides information about the hardware and software requirements for installing Recon as well as the other containerized capabilities

For the most recent version of this guide and other ArcSight documentation resources, visit the [documentation for ArcSight Recon](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the [comment on this topic](#) link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at <https://www.microfocus.com/support-and-services/>.

1 Welcome to ArcSight Recon

Recon provides a modern log search and hunt solution powered by a high-performance column-oriented, clustered database. The [Search](#) feature helps you investigate security issues by viewing search results and identifying outlier events. The [Reports](#) feature, including MITRE ATT&CK content, enables you to [hunt](#) for undetected threats as well as create charts and dashboard to [visualize](#) filtered data with tables, charts, and gauges. With the [Outlier Analytics feature](#) you can identify anomalous behavior by comparing incoming event values to typical values for your environment.

Recon deploys within the **ArcSight Platform**, which provides common services such as the Dashboard and user management.

- ♦ [Investigate alerts and events](#)
- ♦ [Hunt for undetected threats](#)
- ♦ [Analyze anomalous data with outlier analytics](#)
- ♦ [Evaluate and manage the quality of your data](#)
- ♦ [Use visuals and reports to analyze your data](#)
- ♦ [Manage user access](#)

Investigating Events

The **Search** feature enables you to look for and investigate events that meet specified criteria so you can detect anomalies that point to security threats. You can view the results in tabular and timeline formats. Each search consists of [specifying query input](#), [search result fields](#), and the [time period](#) for which you want to search events. Queries are case sensitive. The query input determines the [search type](#) (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests items and operators based on a schema data dictionary. You can also choose from [predefined search queries](#).

- ♦ [Chapter 2, “Searching for Events,” on page 15](#)
- ♦ [Chapter 3, “Managing Your Searches,” on page 21](#)
- ♦ [Chapter 4, “Understanding the Search Parameters,” on page 31](#)

2 Searching for Events

Search is contextual and has an auto-suggest capability to help you specify search criteria and improve productivity. You can retrieve events from an index; search for specific conditions within a rolling time window; create aggregate charts; and identify patterns in your data.

- ♦ [“Understanding the Search Feature” on page 15](#)
- ♦ [“Creating and Saving Searches” on page 16](#)
- ♦ [“Searching Data Stored by ArcSight Logger” on page 18](#)
- ♦ [“Initiating a Search from Enterprise Security Manager” on page 18](#)
- ♦ [“Understanding the Search Progress Indicators” on page 19](#)

Understanding the Search Feature

Recon ingests log data from ArcSight Logger and SmartConnectors routed through Transformation Hub and events from ArcSight Enterprise Security Manager. Each entry in a log is referred to as an **event**. Recon accepts events from Transformation Hub and organizes them to maximize search and storage efficiency.

The **Search** feature enables you to search events by entering a search command, a time window over which to search, and the fields from the Unified Event Schema. Search displays results in an [Events Timeline](#) chart, which a histogram shows the number of events returned over event occurrence time. The [Events table](#) below the Timeline shows events returned by search. When you select an event, Search displays the [Event Details](#) panel.

Search uses a database that serves as the main data store, as well as a cache. The search engine is a scalable server-side application that executes and caches large search queries in the database. In the backend, Recon saves your searches, user preferences, and proxy search requests to the search engine using a REST API. The database stores three [timestamps for each event](#) to provide more clarity in your search results. When [creating a search](#), you specify the timestamp to use for retrieving events.

For the query’s time range, you can choose a fixed start and end date, where you cannot refresh data, or a predefined date range. For example, for the **last 30 minutes** predefined search, you receive updates upon re-executing the search based on the most recent 30 minutes. Alternatively, you could specify [dynamic dates](#), such as **Midnight on the first day of the current month**.

After initiating a search, you can pause, restart, and cancel the process as needed. A [progress bar](#) shows you the percent of retrieved data.

Creating and Saving Searches

Recon supports up to 10 active searches and 40 saved searches per user.

- ♦ [“Create a Search” on page 16](#)
- ♦ [“Save a Search” on page 17](#)
- ♦ [“Name a Search” on page 17](#)
- ♦ [“Find a Saved Search” on page 17](#)

Create a Search

For every search, you must enter the query input, search result fields, and the time period for which you want to search events. Queries are case sensitive. The query input determines the [search type](#) (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries.

If you tend to use the same settings for some search parameters, you might want to [specify a preferred default setting](#). For example, you can configure a default time range.

NOTE: Recon treats a comma (,) between search items and values as an **OR** operator.

1 Select **Search > + New Search**.

You can choose search data [migrated from ArcSight Logger](#).

2 Specify the [query parameters](#).

For example:

```
Source Address = 192.10.11.12 and Destination Address less than  
192.10.11.12
```

Enter # to view the [predefined queries](#).

3 To search for a field without data, enter `[field_name] = Null`.

4 Specify the [fieldset](#) you want for the search results.

By default, Search displays the your [preferred default fieldset](#). If you have not specified one, Search display the Base Event Fields fieldset.

5 For the [time range](#), perform **one** of the following actions:

- ♦ Accept the default time (**Last 30 minutes**)
- ♦ From the drop-down menu, select a pre-defined value under **Quick Ranges**
- ♦ From the drop-down menu, use the **Custom Range** fields to specify a time range
- ♦ From the drop-down menu, select **Dynamic** then enter a [dynamic date value](#)

You can also specify the [timestamp](#) you want to use for the retrieved events. Search uses Normalized Event Time by default.

6 Click **Search**.

Search begins populating the [Events Timeline](#) and [Events table](#). Depending on the number of events retrieved, the search might pause to indicate that the amount of data could impact the search performance. You might want to select a smaller time range. To resume a search, click the play button in the progress bar.

- 7 (Optional) To more easily find the search later, give the search a [name](#).
- 8 To [save](#) the search for future use, select **Save**.

Save a Search

After you execute a search, Recon automatically saves the search if you navigate away from the search page to another Recon feature, the Dashboard, or the Admin pages. However, your search is not automatically saved if you close the browser or tab or when you log out. To permanently save your search, you can add it to the [Saved Searches](#) list.


You can delete the search from the saved list at any time. You can also [configure Search](#) to automatically delete searches after a specific time.

To permanently save your search:

- 1 (Optional) Give the [search a name](#).
- 2 Select **Save**.
- 3 To view your search, select **Saved Searches**.

Name a Search

By default, Recon gives each search the title *Search <N>*. You can apply a custom name to the search at any time.

- 1 When viewing the search, select  beside the search's name.
- 2 Enter the custom name.
- 3 To save your changes, select the **Check** icon.

Find a Saved Search

Select [Search](#) > [Saved Searches](#).

Recon saves up to 40 searches. You can sort the table of saved searches by the search name, query, number of results, or date it was saved. To more easily find searches, you can give them [custom names](#).

Searching Data Stored by ArcSight Logger

You can run ArcSight Logger searches from the Search feature. Logger data (including old events) can be searched using the same parameters as in Search. To do so, an administrator for the ArcSight Database must migrate the information using a Data reader tool to the database from Logger, a process that might require migrations from several loggers as needed.

- ♦ [“Best Practice Considerations for Searching Logger Data” on page 18](#)
- ♦ [“Include Logger Data in a Search” on page 18](#)

For more information about migrating Logger data to the ArcSight Database, see “Logger Search from Recon” in Appendix K of the [Logger Administrator’s Guide](#).

Best Practice Considerations for Searching Logger Data

Before running a search on the Logger data, review the following considerations:

- ♦ Logger data includes live and archived events from local searches. However, it does not include content and configuration data.
- ♦ Search supports only Recon’s specific set of operators.
- ♦ Your searches can include data from Logger’s storage groups even if the Logger storage groups do not display as part of Recon’s configuration. Additional functionalities related to storage groups, like retention policy, is not supported for Logger events.

Include Logger Data in a Search

If Recon and Logger are set to the same timezone, there should be no discrepancy when searching the Logger data.

1. After you migrate data from Logger, select **Search**.
2. From the drop-down list next to the **Search** button, select **Logger**.
3. Add the required query details.
Recon searches for data in the Logger events table in the database.
4. Click **Search**.

Initiating a Search from Enterprise Security Manager

From Enterprise Security Manager (ESM), you can initiate a search in Recon for a maximum of five fields, based on the available columns on the active channel. Within Recon, you can filter ESM data for more specific results. ESM generates a URL, opens a browser, and creates the new search in Recon.

To perform this action, you must enable Recon in ESM. For more information, see the [ESM Installation Guide](#).

Understanding the Search Progress Indicators

As the Search feature retrieves data, it displays a **progress bar** to show its status, including the percent of data received. Rather than attempting to read all data at once, Search gathers data in chunks of time. The progress bar shows the time range from which the results are currently being retrieved.

You can **pause the search** and restart as needed.

NOTE: When performing a search with two or more identical queries the number of events returned for the second search will correspond to the next chunk of data. If you pause then resume the search, the first search will be moved to the next chunk as well, maintaining the same number of events retrieved. The identical queries can contain either one of the built-in queries or a custom query.

3 Managing Your Searches

You can save, refresh, and edit your searches. To help you investigate events, Search displays the results as a [timeline](#), in a [table](#), and in a [detailed view](#). You can export the search results in the table to a CSV file. You can also schedule a search to run at specific intervals, then analyze the completed runs of that search over time.

- ♦ [“Viewing Search Results” on page 21](#)
- ♦ [“Modifying the Search Settings” on page 24](#)
- ♦ [“Exporting the Search Results” on page 24](#)
- ♦ [“Scheduling Regular Runs of a Search” on page 24](#)
- ♦ [“Managing Completed Runs of a Scheduled Search” on page 28](#)

Viewing Search Results

Search displays results in an **Events Timeline**, **Events** table, and **Event Details** panel. If connectors are configured to send raw events, the table and details panel can include **raw event data**. Also, the [maximum number](#) of events that a search can return is 10 million. If your searches regularly stop at the maximum limit, consider splitting the query into separate searches.

- ♦ [“View the Events Timeline” on page 21](#)
- ♦ [“View the Events Table” on page 21](#)
- ♦ [“View and Use the Details of an Event” on page 23](#)
- ♦ [“Identify Fields without Data” on page 23](#)
- ♦ [“Refresh Search Results” on page 23](#)
- ♦ [“Build a Report Using Search Results” on page 24](#)

View the Events Timeline

The **Events Timeline** displays data points in a segmented timeline across the specified time range. The time range in the Timeline corresponds with the data listed in the [Events table](#). If you have a large number of data points or a wide time range, you can see the big, overall picture, but you might not be able to clearly identify specific data points. To **narrow the scope** of the displayed data, select **Enable Range Selector** then adjust the boundaries of the selector.

To view the **details of a data point** or moment in time, select **Disable Range Selector**, and then hover over the data point.

View the Events Table

The **Events** table contains all the fields specified in the [fieldset](#). You can choose to display the table in **Grid View** or **Raw View**. To [view details of a specific event](#), select the event. While viewing the table, you can perform the following actions:

View all details for an event

When you select an event in the table, Search opens the **Event Details panel**. Within the panel, you can further expand the fields for more information.

View raw event data

When you select the **Raw View** icon, the Events table replaces the fieldset columns with a Raw Data column, which displays the whole raw syslog event.

Although the Raw Event field is most applicable for syslog events, you can also display the raw event associated with CEF events. To do so, make sure the connector that is sending events to the database populates the *rawEvent* field with the raw event.

View all event data for a field value

Right-click a value in a table row, then select **Search For**.

Search displays all of the event data based on the selected field value.

View the most and least common values for an event record field

Right-click a column heading, then select **Preview Top/Bottom**.

To help filter data for security threats, you can quickly display the most and least common values for a field. Search displays the count and percentage of hits for the value.

For example, the *Device Vendor* field might have a top value of “bluecoat” with a count of 3,000 hits, accounting for 30 percent of 10,000 results.

View authenticated users

*Applies only when the fieldset for the original search includes the **Device Receipt Time** field.*

Right-click an IP address or host name, then select **Get Authenticated Users**.

Search displays users who have successfully authenticated to the IP address or host name in the last 24 hours.

Copy a value from an event

To use a value from an event elsewhere, simply right-click and copy the value.

Search for an event value

To add a value from an event to your query, right-click the value.

Compare data in columns

Right-click a column heading, then select **Pin Column** or **Unpin Column**.

By pinning a column, you can compare the column’s values against those of other columns.

Search moves the pinned column to the extreme left location in the table. You can pin multiple columns.

Remove or hide columns

If you do not want to view a column, right-click the column heading, then select **Hide Column**.

Alternatively, you can select the **Wrench** icon, and then select the column.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Sort the data in columns

Select the up or down arrow in the column heading to change the sort order.

View and Use the Details of an Event

When you select an event in the [Events table](#), Search opens the **Event Details** panel. In this panel, you can scroll through the specific details of the event. Search groups the details by categories such as **Agent** and **Source**. You can view the raw data details for the event, as well as instruct the panel to include fields with *null* data. For example, you could view details about the agent, category, device, source, or severity. Details displayed in blue text are part of the query filter.

- ♦ [“Export All or Some Event Details” on page 23](#)
- ♦ [“Apply Event Details to Other Searches or Share with Colleagues” on page 23](#)

Export All or Some Event Details

You might want to share the selected event’s details with a colleague or use the details in a report or other media. You can export all content in the Event Details panel with or without empty values.

Apply Event Details to Other Searches or Share with Colleagues

Search allows you to copy the URL of a detail to share with colleagues or open in a separate browser tab. You can also choose to use the detail in a new search query and in an nslookup or Whois search. For example, you might select a domain name and use a nslookup to check whether the domain is valid.

Identify Fields without Data

If an event does not have data for a schema field, Search represents the absence of data (*null*) in the results in the following ways:

Affected Field	Displayed Result
Search field	Null, NULL and null query formats
Events table	Empty cell
Empty field from ESM (for example, <code>name= ' '</code>)	<code>name = "</code> , NULL
Event Details pane	--- in the cell

Refresh Search Results

If the [time range](#) for your search is based on a predefined range, such as **Last 30 minutes**, you can refresh the search results as desired. However, refreshing the browser as you update a search does not save your changes. You must [save the refreshed results](#).

Build a Report Using Search Results

Search assigns a unique **Search Results ID**, which is a link to the temporary table containing the search results that you see in the [Events table](#). You can copy the ID to build a report around those events. You can also build a report based on the Search Results ID for a [completed run](#) of a scheduled search.

- 1 In the table's header, select the **Copy** icon.
- 2 (Optional) To view or save the copied ID, paste the ID in a text editor.
- 3 Select **Reports > Designer**.
- 4 For **Select a data source**, paste the copied ID.
- 5 Complete the report design.

Modifying the Search Settings

When viewing a search, you can change the query, a fieldset, and the range selector.

- 1 In the saved search, change the [query](#), [fieldset](#), or [time range](#).
- 2 To return to your original settings, select **Revert Changes**.
- 3 To update the search results with the modified settings, select **Search Now** or **Search**.

Exporting the Search Results

You can export the [Events table](#) to a CSV file.

- 1 In the table's header, select the **CSV** icon.
- 2 Choose to save the file or open in a desired application.

Search exports data based on the specified [fieldset](#) for the search. The export process limits the file to one million event records.

Scheduling Regular Runs of a Search

Select **Search > Scheduled Searches > Schedule**.

*You must have the **Scheduled Search** permission to schedule runs of a search.*

A **scheduled search** is a search that runs on a regular interval. Whereas a [saved search](#) is saved, but does not run automatically.

Each time a scheduled search runs, search adds the results to the list of [Completed Searches](#) runs.

- ♦ [“Create a Scheduled Search” on page 25](#)
- ♦ [“View Scheduled Searches” on page 26](#)
- ♦ [“Clone a Scheduled Search” on page 27](#)
- ♦ [“Edit a Scheduled Search” on page 27](#)

- ♦ “Delete a Scheduled Search” on page 27
- ♦ “Enable and Disable a Scheduled Search” on page 27

Create a Scheduled Search

Before creating a [Scheduled Search](#), you must [create or save](#) at least one search. For every scheduled search, enter the [query](#), [fieldset](#), or [time range](#) for the search events or leave the defined values for the saved search. Just as for a saved search, the following considerations apply to a scheduled search:

- ♦ The search is case sensitive.
- ♦ The query input determines the [search type](#) (full text, natural language, or contextual).
- ♦ As you specify the search criteria, the system suggests search items and operators based on a schema data dictionary. To view the [predefined queries](#), type # in the query field.
- ♦ To search for a field without data, enter `[field_name] = Null`.
- ♦ The system treats a comma (,) between search items and values as an **OR** operator.

To create a scheduled search:

- 1 (Conditional) To schedule a search that you are currently viewing, select **Schedule**.
- 2 (Conditional) To schedule a search without currently viewing one, complete the following steps:
 - 2a Select **Search > Scheduled Searches**.
 - 2b Select **+**.
- 3 Specify a **Name** that is 5 to 255 character long.
- 4 To enable the scheduled search, select the **Status** box.
You can enable and disable scheduled searches at any time in the **Scheduled** tab.
- 5 To indicate how frequently you want the search to run, specify one of the following options:
 - ♦ **Hourly**
 - ♦ **Daily**
 - ♦ **Weekly**
 - ♦ **Monthly**
- 6 Depending on the frequency that you specified in [Step 5](#), configure the settings for the dates and times of each run.

NOTE: For **Starting from**, if you select **end after**, the maximum number of instances is 1000.

- 7 (Conditional) To schedule an existing search, select one from the pull-down menu under **Search Query and Metadata**.
- 8 (Conditional) To create a query, specify the [query parameters](#), [fieldset](#), and [time range](#).

For example:

```
Source Address = 192.10.11.12 and Destination Address less than
192.10.11.12
```

- 9 Under **Result Retention and Limitations**, configure how long you want to keep each completed run of the scheduled search.

NOTES:

- ♦ Your choice of values for each setting might be confined to limits set by your product administrator.
- ♦ For **Delete results after**, you can specify a value that overrides how you configured **Search Expires In** for your search preferences. For example, you prefer that searches expire within five days. But you want the results for this scheduled search to expire after 10 days.
- ♦ (Conditional) If you have the *Never Expire Search Results* permission, you can choose **Never Expire** to retain the search results indefinitely.
- ♦ If you select **Keep only the most recent run**, then, when a run completes successfully, Search deletes the results of the previous run.

- 10 For **Retrieve up to**, specify the number of results you want to receive.

- 11 Select **Schedule**.

View Scheduled Searches

The **Scheduled Searches** tab displays information for created scheduled searches. You can perform the following actions:

View and edit all details for a schedule search

To view specific scheduled search details, in the Name column, locate the search name and select it. Click **Edit** at the top of the table.

Sort the data in columns

To change the sort order, click the column heading to toggle between ascending and descending order.

Reorder columns

To rearrange the order of the columns, drag each column header to a new position.

Search for a search keyword

To find a keyword, click the field next to the **Magnifying Glass** icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the **Wrench** icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

You can filter scheduled searches based on Status, Timestamp, and Fieldset. To filter the data for more specific results, in the far-right corner of the window, click the **Funnel** icon (Filters), and then select and clear the filter options.

Clone a Scheduled Search

After creating a scheduled search, you can clone it at any time.

- 1 Select **Search > Scheduled Searches**.
- 2 Select the scheduled searches that you want to clone.
- 3 Click the **clone** icon.

Edit a Scheduled Search

After creating a scheduled search, you can edit it at any time. After you modify a schedule, the first completed run will have a flag to indicate that the modification occurred.

- 1 Select **Search > Scheduled Searches**.
- 2 Select the scheduled searches that you want to edit.
- 3 Click the **edit** icon.

If you change the **Pattern** values, please be aware that Search counts any and all completed runs before you made the change. For example, your scheduled search uses the **repeat forever** option and Search has performed three runs. If you update the **ending option** to end after eight occurrences, Search counts the three previous completed runs; therefore, you would only have five occurrences of the eight occurrences left to run. Should you want eight occurrences, you would need to change your **ending option** to 11 occurrences.

Delete a Scheduled Search

You can delete a scheduled search at any time. After selecting **Delete**, the system prompts you to keep or delete the **completed runs** associated with the scheduled search.

NOTE: To cancel the deletion process, select the **X** that closes the dialog box, instead of selecting **Yes** or **No**.

Enable and Disable a Scheduled Search

After creating a scheduled search, you can enable and disable it at any time.

- 1 Select **Search > Scheduled Searches**.
- 2 Select the searches that you want to enable or disable.
- 3 Select **Enable** or **Disable**.

The **Status** column, if selected in the **Manage Columns** option, displays the status of either  **Enabled** (green) or **X Disabled** (red).

Managing Completed Runs of a Scheduled Search

Select **Search** > **Scheduled Searches** > **Completed**.

You must have the **Scheduled Search** permission to schedule searches.

After creating a **scheduled search**, you can view, delete, export, and filter the **completed runs** of that search. The results of a completed run are immutable. That is, if you edit the settings or query of a completed run, your changes do not affect the original results stored in the Completed list of scheduled searches.

- ♦ [“View a Completed Run of a Scheduled Search” on page 28](#)
- ♦ [“Delete Completed Runs of a Scheduled Search” on page 29](#)
- ♦ [“Export Completed Runs of a Scheduled Search” on page 29](#)

View a Completed Run of a Scheduled Search

Select **Search** > **Scheduled Searches** > **Completed**.

The name of a completed run represents the name of the scheduled search name plus its start date and time. Search groups all completed runs of the same scheduled search under that scheduled search. When a run is in progress, Search displays the number of events received thus far and when the last chunk of data was received. Also, a flag beside the name of a completed run indicates that the settings for that scheduled search were changed before this run.

In the **Completed** tab, you can perform the following actions:

View all details for a completed schedule search

To view completed search results, click the **Eye** icon beside the search name.

Sort the data in columns

To change the sort order, click the column heading.

Reorder columns

To rearrange the order of the columns, drag each column to new position.

Search for a search keyword

To find a keyword, click in the field next to the **Magnifying Glass** icon (Search Keyword), enter a value, and the system displays your results automatically.

Hide and display columns

To hide and display a column, in the far right-corner of the window, click the **Wrench** icon (Manage Columns), and then select and clear the column name checkboxes.

Filter the data in columns

To filter scheduled searches based on *Status* and *Fieldset*, select the corresponding filter parameter. You can also filter completed scheduled searches based on a time range (custom and preset).

To filter the data for more specific results, in the far right-corner of the window, click the **Funnel** icon (Filters), and then select and clear the filter options. To filter the results based on execution time, set the date picker filter in the far right corner.

Create a report based on the run results

Each completed run has a unique [Search Results ID](#), which allows you to create a report based on the search results.

To copy the ID, [view](#) the search results. Then either copy the ID from the URL or select the **Copy** icon above the Events table. To complete the process, follow the steps in “[Build a Report Using Search Results](#)” on page 24.

Delete Completed Runs of a Scheduled Search

You can delete a completed run of a scheduled search at any time.

- 1 Select **Search** > **Scheduled Searches** > **Completed**.
- 2 Select the completed runs that you want to delete.
- 3 Click the **delete** icon.

Export Completed Runs of a Scheduled Search

You can export the completed run of a scheduled search to CSV format.

- 1 Select **Search** > **Scheduled Searches** > **Completed**.
- 2 Click the **CSV** icon next to the name of the scheduled search that you want to export.
- 3 Alternatively, view the search, then select the **CSV** icon to export the results.

4 Understanding the Search Parameters

To search for events or alerts, you specify the [query input](#), the [search result fields](#), and the [time period](#). The query input determines the search type (full text, natural language, or contextual). As you specify the criteria for a search query, Search suggests search items and operators based on a schema data dictionary. You can also choose from predefined queries and specify default settings.

- ♦ [“Understand the Types of Search Queries” on page 31](#)
- ♦ [“Using GlobalEventID in a Query” on page 33](#)
- ♦ [“Understand the Query Syntax, Operators, and Functions” on page 33](#)
- ♦ [“Specify a Group of Fields” on page 43](#)
- ♦ [“Specify an Alias for a Field” on page 44](#)
- ♦ [“Specify IP Addresses and Subnets” on page 47](#)
- ♦ [“Include a Storage Group’s Filter in the Search Query” on page 49](#)
- ♦ [“Extend the Search with a Lookup List” on page 49](#)
- ♦ [“Use Specific Sets of Fields for Search Results” on page 51](#)
- ♦ [“Configure the Time Range” on page 54](#)
- ♦ [“Configure Preferred Settings for Searches” on page 56](#)

Understand the Types of Search Queries

Search supports the following types of search queries:

FULL TEXT SEARCH

Searches across all columns using a ‘contains’ operation to determine if the value is found.

Syntax	Example
<value>	ssh

FIELD-BASED SEARCH

Searches based on the field and operator designation to determine if the value is found in the specified field.

Your search can reference fields with the Unified Schema to either retrieve the field in results, apply a filter criteria or create a user defined expression. The **Unified Schema** defines a consistent event model that can be used across all of ArcSight family of products.

Syntax	Example
<key> <operator> <value>	sourceAddress = 10.0.111.5

HASHTAG (predefined searches)

The Search feature includes several predefined queries out-of-the-box. In the query field, enter a hashtag, and then select the criteria to use. In addition to these predefined searches, you can use the session searches and save searches in the input field using a hashtag prefix.

This predefined query...	Uses this search criteria...
#Configuration Changes	categoryBehavior = /Modify/Configuration AND categoryOutcome = /Success
#DGA Events	deviceCustomNumber1 >= 1 AND deviceCustomNumber1Label contains DNS
#DNS Events	deviceEventCategory = PACKET
#DoS Events	#Category Technique = /DoS
#ESM Correlation Events	Type=Correlation
#Failed Logins	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success
#Failed Logins For User \$Username	Category Behavior = /Authentication/Verify AND categoryOutcome != /Success for user <username>
#Firewall Events	categoryDeviceGroup = /Firewall
#Firewall Drop	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/ Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure
#Firewall Drop For \$Ip	categoryDeviceGroup = /Firewall AND categoryObject starts with /Host/ Application/Service AND (categoryBehavior starts with /Access OR categoryBehavior = /Communicate/Query) AND categoryOutcome = /Failure for <IP_address>
#Malicious Code Activity	categoryObject STARTS WITH /Vector, /Host/Infection, /Host/ Application/Malware OR categoryObject = /Host/Application/DoS Client, /Host/Application/Backdoor OR categoryTechnique STARTS WITH /Code
#MITRE ATT&CK Events	Device Custom String1 Label ='MITRE ID'
#Proxy Events	Category Technique=/Proxy
#SSH Authentication	categoryBehavior = /Authentication/Verify AND destinationUserName != Null and contains ssh
#VPN Connections	categoryDeviceGroup = /VPN AND Category Behavior = /Authentication/ Verify AND categoryOutcome = /Success AND destinationUserName != Null
#Vulnerabilities Events	Category Technique= /scanner/device/vulnerability
#Windows Account Creation	deviceVendor = Microsoft AND deviceEventClassId = Microsoft-Windows-Security-Auditing:4720, Security:624

This predefined query...	Uses this search criteria...
#Windows New Service Created	(deviceEventClassId='Microsoft-Windows-Security-Auditing:4697' or deviceEventClassId=' Service Control Manager:7045') and deviceProduct='Microsoft Windows'

Using GlobalEventID in a Query

To help you identify an event that might be seen by multiple ArcSight components, the connectors assign the event a unique 64-bit ID. To include a GEID in your search query, enter `globalEventID`. You can view the GEID of the event in the Event Details.

For events to have a GEID, use ArcSight Management Center to configure connectors to include the ID. For more information, see the *Administrator's Guide to ArcSight Platform* or the guide for the connector.

Understand the Query Syntax, Operators, and Functions

Search supports a variety of search operators and functions.

The search query bar automatically displays related fields and operators as you enter your query. For example, type the word “domain” to see all available fields that might contain that string or name. Type an integer like “22”, and Search displays a list of fields to choose from, such as Destination Port, Source Port or “any port.”

You can also specify a [storage group](#) in the query.

- ♦ [“Understand the Query Syntax Requirements” on page 33](#)
- ♦ [“Understand the Search Query Functions and Operators” on page 36](#)
- ♦ [“Understand the Functions for Building Eval Expressions” on page 37](#)

Understand the Query Syntax Requirements

Depending on the [type of search](#) you create, the query must meet the requirements listed in the following table. Also, Search treats a comma (,) between search items and values as an **OR** operator.

By default, Search is case-sensitive to support faster performance. However, you can instruct the database to support case-insensitive searches. For more information, see the [Administrator's Guide to ArcSight Platform](#).

Type	Full-text	Field-based	Hashtag (predefined)
Case sensitivity	Case-sensitive	Case-sensitive	Case-insensitive

Type	Full-text	Field-based	Hashtag (predefined)
Exact Match	<p>Keyword treated as keyword*.</p> <p>Example: /Execute matches: / Execute, /Execute/ Start, /Execute/ Response,/Execute/ Query</p>	<p>Enclose value in double quotes.</p> <p>Example: Category Behavior ="/Execute"</p>	n/a
Nesting, including parenthetical clauses, such as (a OR b) AND c	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords.</p>	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords.</p>	<p>Allowed</p> <p>Use Boolean operators to connect and nest keywords</p>
Implicit Operators	<p>When you enter two values separated by a space, this is treated as an implicit AND condition.</p> <p>Example: ssh fail</p>	<p>The AND/OR treatment depends on the operator used in the search.</p> <p>For example, destinationAddresses = 1.1.1.1, 2.2.2.2 is equivalent to destinationAddresses = 1.1.1.1 or destinationAddresses = 2.2.2.2,</p> <p>while the query destinationAddresses != 1.1.1.1, 2.2.2.2 is equivalent to destinationAddresses != 1.1.1.1 and destinationAddresses != 2.2.2.2</p>	n/a

Type	Full-text	Field-based	Hashtag (predefined)
List Operations	n/a	<p>Performs an inner join or a left join against a custom list.</p> <p><i>Syntax for an Inner Join:</i> source address in list CustomListName_CustomColumnName</p> <p><i>Syntax for a Left Join:</i> source address not in list CustomListName_CustomColumnName</p>	n/a
Time Format (when searching for events that occurred at a particular time)	<p>No specific format</p> <p>The query needs to contain the exact timestamp string.</p> <p>Example: "10:34:35"</p>	<p>YYYY-MM-DD YYYY-MM-DD HH:mm YYYY-MM-DD HH:mm:ss.fff</p> <p>To narrow the time range, use the following operators:</p> <ul style="list-style-type: none"> ♦ in between (><) ♦ greater than (>) ♦ less than (<) 	n/a
Special Characters: \ * ' "	Use the backslash (\) as an escape character.	Use the backslash (\) as an escape character.	n/a
Wildcard	<p>Can appear anywhere in the value.</p> <p>Examples: *log log* lo*g*</p> <p>Searches for ablog, blog, long, etc.</p>	<p>Can appear anywhere in the field.</p> <p>Examples: name=*log Searches for ablog, blog, etc. in name field name="\"*log" name=*log Both search for *log</p>	n/a
Escape a Wildcard Character	<p>Can search for * by escaping the character.</p> <p>Example: log*</p>	<p>Can search for * by escaping the character.</p> <p>Example: name=log*</p>	n/a

Understand the Search Query Functions and Operators

You can specify the following search operators in the query:

Operator	Alternative Operator	Examples
AND		#Firewall drop and sourceAddress equals 10.0.112.9 sourceAddress equals 10.0.112.9 and destinationAddress = 10.0.116.148
OR		fail OR ssh destinationAddress = 10.0.111.5 OR destinationAddress=10.0.116.148 destinationAddress =10.0.111.5, 10.0.116.48
not equal	<> !=	destinationPort not equal 21
equals	= == is equal to equal	name equals INVALID password device vendor equals CISCO
greater than	> is greater	bytes In greater than 100
less than	< is less is lower less	bytes out less than 1000
greater equal than	>= gte greater equal	End Time greater equal than 2017-07-25 End Time greater equal than 2017-07-25 09:07 End Time greater equal than 2017-07-25 09:07:43 End Time greater equal than 2017-07-25 09:31:22.685
less equal than	<= lte less equal	Base Event Count less equal than or equal 50
starts with	startswith	message starts with FIN
does not start with		name does not start with FIN
ends with	endswith	message ends with out
does not end with		message does not end with out
contains	contain like has substring	name contains TCP
does not contain	does not have	name does not contain TCP

Operator	Alternative Operator	Examples
in list	match in list of	device vendor equals CISCO and source address in list customListName_customColumnName device vendor equals CISCO and source address in list badGuyIpList_badGuyIp
not in list	not match not in list of	source address not in list customListName_customColumnName source address not in list badGuyIpList_badGuyIp
in subnet	n/a	source address in subnet 10.0.0.0/8
not in subnet	n/a	source address not in subnet 10.0.0.0/8
 (Pipeline operator)	n/a	Combine various search functions separated by the operator: ssh eval test1 = abs (40) ssh eval test1 = sin (Bytes In)
eval <expression> name	n/a	eval URL_Length = length (Request URL)
rename	n/a	rename source address as NewSourceAddress
where	n/a	where Bytes In >= 3000 where Category Outcome = /Success

Understand the Functions for Building Eval Expressions

The Eval function allows you to define and name an expression that is returned in the search. To build an eval expression, you can use the following functions:

- ♦ [“Comparison and Conditional Functions” on page 38](#)
- ♦ [“Cryptographic Function” on page 38](#)
- ♦ [“Informational Function” on page 38](#)
- ♦ [“Mathematical Functions” on page 39](#)
- ♦ [“Statistical Functions” on page 40](#)
- ♦ [“Text Functions” on page 41](#)
- ♦ [“Trigonometry Functions” on page 42](#)

Comparison and Conditional Functions

Function	Description	Example
<code>coalesce(X[, Y, Z, N, ...])</code>	Returns the value of the first non-null expression in the list. If all expressions evaluate to null, then COALESCE returns null. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. <i>X</i> can be a number, field or expression.	<code>... eval newField = coalesce(null, null, 2, 3)</code> <i>Returns: 2</i>
<code>nullif(X, Y)</code>	Compares two expressions. If the expressions are not equal, the function returns the first expression (expression1). If the expressions are equal, the function returns null. <i>X</i> and <i>Y</i> can be a number, field or expression. <i>Y</i> must have same data type that <i>X</i> .	<code>... eval newField = nullif(2, 3)</code> <i>Returns: 2</i> <code>... eval newField = nullif(2, 2)</code> <i>Returns: null</i>

Cryptographic Function

Function	Description	Example
<code>md5(X)</code>	Calculates the MD5 hash of string, returning the result as a string in hexadecimal. <i>X</i> must be a string.	<code>... eval newField = md5('123')</code> <i>Returns:</i> 202cb962ac59075b964b07152d234b70

Informational Function

Function	Description	Example
<code>isnull(X)</code>	Returns true if the <i>X</i> is null otherwise returns false.	<code>... eval newField = isnull(2)</code> <i>Returns: false</i>

Mathematical Functions

Function	Description	Example
abs(X)	Takes a number, X, and returns its absolute value. X can be a number, field or expression.	The function assigns the evaluated value to the new field. If the value of X is 3 or -3, the function assigns the evaluated value of 3 to the field absnum: ... eval absnum=abs(number) ... eval absnum = abs(bytesIn) ... eval absnum = abs(1 - bytesIn)
cbrt(X)	Takes one numeric argument, X, and returns its cube root.	... eval n=cbrt(2) <i>Returns: 8</i>
ceiling(X)	Rounds a number, X, up to the next highest integer. X can be a number, field or expression.	... eval n=ceil(1.9) ... eval n=ceiling(1.9) <i>Returns: n=2</i>
exp(X)	Takes a number, X, and returns e^X . X can be a number, field or expression.	... eval y=exp(3) <i>Returns: y=20.0855369231877</i>
floor(X)	Rounds a number, X, down to the nearest whole integer. X can be a number, field or expression.	... eval n=floor(1.9) <i>Returns: 1</i>
mod(X, Y)	Returns the modulo of X and Y. ($X\%Y$; the remainder of X divided by Y.)	... eval newField = mod(25,10) <i>Returns: 5</i>
power(X,Y)	Returns a value representing one number raised to the power of another number. X is the base and Y the exponent. X and Y can be a number, field or expression.	... eval newField = power(2, 3) <i>Returns: 8</i>
round(X, Y)	Rounds X to the nearest integer. Y is the precision to use, if omitted the default precision is zero. X can be a number, field or expression. Y is a numeric value to indicate the precision.	... eval n=round(1.4) <i>Returns: 1</i> ... eval n=round(1.5) <i>Returns: 2</i>

Function	Description	Example
sign(X)	Returns a value of -1, 0, or 1 representing the arithmetic sign of the argument.	... eval newField = sign(-8.4) <i>Returns: -1</i> ... eval newField = sign(4) <i>Returns: 1</i> ... eval newField = sign(0) <i>Returns: 0</i>
sqrt(X)	Takes one numeric argument, X, and returns its square root. X can be a number, field or expression.	... eval n=sqrt(9) <i>Returns: 3</i>
trunc(X,Y)	Returns the expression value truncated (toward zero). X can be a number, field or expression. Y is a numeric value to indicate the precision.	... eval newField = trunc(1.9) <i>Returns: 1</i> ... eval newField = trunc(2.89999, 2) <i>Returns: 2.89</i>

Statistical Functions

Function	Description	Example
greatest(X,Y[,Z,N, ...])	Returns the largest value in a list of expressions. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. X can be a number, field or expression.	... eval newField = greatest(7, 5, 9) <i>Returns: 9</i> ... eval newField = greatest('sit', 'site', 'sight') <i>Returns: site</i> ... eval newField = greatest(bytesIn, 100) <i>Returns: 100, when bytesIn is less than 100</i>
least(X,Y[,Z,N, ...])	Returns the smallest value in a list of expressions. The list is up to 20 elements long. In the list of expressions all elements must be of same type. The only supported types are numeric and string. X can be a number, field or expression.	... eval newField = least(7, 5, 9) <i>Returns: 5</i> ... eval newField = least('sit', 'site', 'sight') <i>Returns: sight</i> ... eval newField = least(bytesIn, 100) <i>Returns: 100, when bytesIn is greater than 100</i>

Function	Description	Example
randomint(<i>X</i>)	Returns a random number between 0 and <i>X</i> -1. <i>X</i> can be any positive integer between the values 1 and 9,223,372,036,854,775,807.	... eval newField = randomint(10) <i>Returns:</i> a random number between 0 and 9

Text Functions

Function	Description	Example
length(<i>X</i>)	Returns the character length of a string, <i>X</i> eval n=length(field) <i>Returns:</i> the length of (field). If the field is 256 characters long, it returns n=256. ... eval n=length("abc") <i>Returns:</i> n=3 (abc is a literal string, surrounded by double quotes)
lower(<i>X</i>)	Takes a string argument, <i>X</i> , and returns the lowercase version.	... eval name=lower("USERNAME") ... eval name=tolower("USERNAME") <i>Returns:</i> the value of the field username in lowercase. If the username field contains FRED BROWN, it returns name=fredbrown.
substr(<i>X</i> , <i>Y</i> , <i>Z</i>)	This function returns a new string that is a substring of string <i>X</i> . The substring begins with the character at index <i>Y</i> and extends up to the character at index <i>Z</i> -1. The index is a number that indicates the location of the characters in string <i>X</i> , from left to right, starting with zero. <i>Y</i> can be negative. <i>Z</i> cannot be negative.	... eval n=substr("ArcSight", 5, 6) <i>Returns:</i> "g" ... eval n=substr("ArcSight", 2, 6) <i>Returns:</i> "cSig" ... eval n=substr("ArcSight", 0, 3) <i>Returns:</i> "Arc"

Function	Description	Example
trim(<i>X</i>) ltrim(<i>X</i>) rtrim(<i>X</i>)	trim(<i>X</i>) removes all spaces from both sides of the string <i>X</i> . ltrim(<i>X</i>) removes all spaces from the left side of the string <i>X</i> . rtrim(<i>X</i>) removes all spaces from the right side of the string <i>X</i> .	For the sake of these examples, assume that <i>X</i> is a literal string and <i>_</i> represents any number of space characters. ... eval trimmed=ltrim("_string_") <i>Returns:</i> trimmed="string_" ... eval trimmed=rtrim("_string_") <i>Returns:</i> trimmed="_string" ... eval trimmed=trim("_string_") <i>Returns:</i> "string"
upper(<i>X</i>)	Takes one string argument and returns the uppercase version.	... eval name=upper("username") ... eval name=toupper("username") <i>Returns:</i> the value of the field username in uppercase. If username contains fred brown, it returns name=FRED BROWN.

Trigonometry Functions

Function	Description	Example
acos(<i>X</i>)	Takes one numeric argument, <i>X</i> , and returns its trigonometric inverse cosine.	... eval newField = acos(0.3) <i>Returns:</i> 1.2661036727795
asin(<i>X</i>)	Takes one numeric argument, <i>X</i> , and returns its trigonometric inverse sine.	... eval newField = asin(3) <i>Returns:</i> 0.304692654015398
atan(<i>X</i>)	Takes one numeric argument, <i>X</i> , and returns its trigonometric inverse tangent.	... eval newField = atan(3) <i>Returns:</i> 0.291456794477867
atan2(<i>X</i> , <i>Y</i>)	Returns a value representing the trigonometric inverse tangent of the arithmetic dividend of the arguments.	... eval newField = atan2(2,1) <i>Returns:</i> 1.10714871
cos(<i>X</i>)	Takes one numeric argument, <i>X</i> , and returns its trigonometric cosine.	... eval newField = cos(3) <i>Returns:</i> 2435538

Function	Description	Example
cosh(X)	Takes one numeric argument, X, and returns its hyperbolic cosine.	... eval newField = cosh(3) <i>Returns:</i> 10.0676619957778
cot(X)	Takes one numeric argument, X, and returns its trigonometric cotangent.	... eval newField = cot(3) <i>Returns:</i> -7.01525255143453
ln(X)	Takes a number, X, and returns its natural log. X can be a number, field or expression.	... eval lnBytes=ln(bytesIn) <i>Returns:</i> the natural log of the value of "bytesIn". If "bytesIn" contains 100, returns 4.605170186.
log(X, Y)	Returns the logarithm to the specified base of the argument. X is the base and Y can be a number, field or expression. X is optional. If not specified, it will take 10 as the default value.	... eval test1= log (10,2) <i>Returns:</i> 0.301 ... eval test1 = log (2) <i>Returns:</i> 0.301 as it takes the default base as 10
log10(X)	(Evaluates the log of number X with base 10. X can be a number, field or expression.	... eval num=log10(10000) <i>Returns:</i> 4
sin(X)	Takes one numeric argument, X, and returns its trigonometric sine.	... eval newField = sin(3) <i>Returns:</i> 0.141120008059867
sinh(X)	Takes one numeric argument, X, and returns its hyperbolic sine.	... eval newField = sinh(3) <i>Returns:</i> 10.0178749274099
tan(X)	Takes one numeric argument, X, and returns its trigonometric tangent.	... eval newField = tan(3) <i>Returns:</i> -0.142546543074278
tanh(X)	Takes one numeric argument, X, and returns its hyperbolic tangent.	... eval newField = tanh(3) <i>Returns:</i> 0.99505475368673

Specify a Group of Fields

Search enables you to quickly select fields that have common groupings. In the query, you can specify a **group alias** that displays all fields or columns associated with the group. The following table provides some common group aliases.

Group Alias	Includes a list of these fields or columns...
category	All category fields
custom float	All custom float fields
domain	All domain fields

Group Alias	Includes a list of these fields or columns...
hostname	All hostname columns
id	All ID columns
ip	All IP address columns
ip6	All IPv6 address columns
label	All label columns
mac	All MAC address columns
path	All path columns
port	All port columns
timestamp or time	All time columns (device receipt time, agent receipt time)
uri	All URI columns
url	All URL columns
username or user	All user columns

Specify an Alias for a Field

In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. For the fields shown in the following table, you can also use the **presentable field names**, such as Agent Address. Search suggests presentable names.

Field	Aliases
agentAddress	agt agent ip
agentHostName	ahost
agentId	aid
agentMacAddress	amac agent mac
agentReceiptTime	art
agentTimeZone	atz
agentTranslatedAddress	agent translated ip
agentType	at
agentVersion	av
applicatonProtocol	app protocol
baseEventCount	cnt

Field	Aliases
bytesIn	in
bytesOut	out
categoryBehavior	behavior
categoryDeviceGroup	device group
categoryObject	object
categorySignificance	significance
categoryTechnique	technique
destinationAddress	dst destination ip destinationip dst ip dest ip target ip targetip target
destinationHostName	dhost destination name
destinationMacAddress	dmac destination mac
destinationNtDomain	dntdom
destinationPort	dpt destination port dstport dest port targetport target port
destinationProcessId	dpid
destinationProcessName	dproc
destinationTranslatedAddress	destination translated ip
destinationuserId	duid
destinationUserName	duser dst user dest user destination user dst usr
destinationUserPrivileges	dpriv
deviceAction	act

Field	Aliases
deviceAddress	dvc deviceaddr deviceip device ip
deviceCustomFloatingPoint n	cfpn
Valid values for n are integers between 1 and 4 For example: deviceCustomFloatingPoint1	For example: cfp1
deviceCustomFloatingPoint n Label	cfpnLabel
Valid values for n are integers between 1 and 4 For example: deviceCustomFloatingPoint1Label	For example: cfp1Label
deviceCustomIPv6Address n	c6an device custom ipv6 n
Valid values for n are integers between 1 and 4 For example: deviceCustomIPv6Address2	For example: c6a2
deviceCustomIPv6Address n Label	c6anLabel
Valid values for n are integers between 1 and 4 For example: deviceCustomIPv6Address2Label	For example: c6a2Label
deviceCustomNumber n	cn n
Valid values for n are integers between 1 and 3 For example, deviceCustomNumber3	For example: cn3
deviceCustomNumber n Label	cn n Label
Valid values for n are integers between 1 and 6 For example: deviceCustomNumber6Label	For example: cn6Label
deviceCustomString n	Cs n
Valid values for n are integers between 1 and 6 For example: deviceCustomString5	For example: Cs5
deviceEventCategory	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	dtz
deviceTranslatedAddress	device translated ip
endTime	end
eventOutcome	outcome

Field	Aliases
fileName	fname
fileSize	fsize
message	msg
requestUrl	request URL
sourceAddress	src source ip sourceip src ip
sourceHostName	shost
sourceMacAddress	smac source mac
sourceNtDomain	sntdomain
sourcePort	spt srcport src port
sourceProcessId	spid
sourceProcessName	sproc
sourceTranslatedAddress	source translated ip
sourceUserId	suid
sourceuserName	suser src user source user src usr
sourceUserPrivileges	spriv
startTime	start
transportProtocol	proto

Specify IP Addresses and Subnets

Your query can include IPv4, IPv6, and MAC addresses.

- ♦ [“How Search Stores IP and MAC Addresses” on page 48](#)
- ♦ [“Enter an IP or MAC Address” on page 48](#)

How Search Stores IP and MAC Addresses

Search stores IPv4, IPv6, and MAC addresses in a format that provides search flexibility and enables you to perform the following actions:

Compare IP addresses for optimum performance

For example, `Agent Address > 192.10.11.12`.

Specify a range of IP addresses

For example, you can enter the following types of queries:

- ♦ `Agent Address in between 192.2.13.1 and 192.2.13.11`
- ♦ `Source Address greater equal than 192.10.11.12`
- ♦ `Destination Address less than 192.112.98.33`

Use abbreviated input search notation

You can enter the following types of queries:

- ♦ To specify IP addresses in the subnet starting with a particular value:

`Agent Address in subnet 192.*`

- ♦ To specify an IPv4 address in a subnet that uses CIDR notation. The first eight bits are the network part of the address, leaving the last 24 bits for specific host addresses.

`Agent Address in subnet 192.0.0.0/8`

- ♦ To specify an agent address in a subnet that uses CIDR notation. The first 24 bits are the network part of the address, leaving the last 40 bits for specific host addresses.

`Agent Address in subnet 2001:0db8:0000:0000:0000:ff00:0042:8329/24`

Search stores MAC addresses in their original format.

Enter an IP or MAC Address

You can enter IP addresses in the following formats:

- ♦ `aa:aa:aa:aa:aa:aa`
- ♦ `aa-aa-aa-aa-aa-aa`

The following table lists the query format and examples for the type of IP address.

Type of address	Format in a query...	Examples
IPv4	a.b.c.d	a.*
		a.b.*
		a.b.c.*
		a.b.c.d/8
IPv6	Full form	2001:0db8:0000:0000:0000:ff00:0042:8329
	Canonical form without leading zeroes in each group	2001:db8:0:0:0:ff00:42:8329

Type of address	Format in a query...	Examples
IPv6 in a subnet	Canonical form without consecutive sections of zeroes	2001:db8::ff00:42:8329
	Include CIDR notation	2001:0db8:0000:0000:0000:ff00:0042:8329 2001:0db8:0000:0000:0000:ff00:0042:8329/24 2001:db8::/32
		NOTE: For the 2001:db8::/32 format, you can omit part of the IPv6 address, depending on the subnet that you are querying.
MAC	a:b:c:d:e:f	94:18:82:6D:63:74
	a-b-c-d-e-f	94-18-82-6D-63-74

Include a Storage Group's Filter in the Search Query

Search allows you to include a [storage group](#) in a query. For example, you have a storage group called *Firewall Events* that has the following query: `categoryDeviceGroup='/Firewall'` or `categoryDeviceGroup='/IDS'`. Rather than entering that query again in Search, specify the following for your Search query: `storageGroup=Firewall Events`.

IMPORTANT: For best results, specify the storage group at the beginning of the Search query.

Extend the Search with a Lookup List

Select [Configuration](#) > [Lookup Lists](#).

You can create CSV files, or **lookup lists**, that enables the Search feature to create additional tables with different fields and store them in the database. You can add lookup list fields to [fieldsets](#) and use them in search queries.

- ♦ [“Considerations for the Lookup List File” on page 49](#)
- ♦ [“Create a Lookup List” on page 50](#)
- ♦ [“Replace a Lookup List” on page 51](#)
- ♦ [“Delete a Lookup List” on page 51](#)

Considerations for the Lookup List File

The CSV file for your lookup list must meet the following requirements:

- ♦ The first row must be a comma-separated list of field names.

The field names cannot exceed 40 characters. The names can only contain alphanumeric characters and underscores. They must start with an alpha character.

- ♦ The remaining rows must be comma-separated values for the fields in the first row.
- ♦ All rows must contain the same number of values.
- ♦ You must select one of the columns as the **key field**, and the values of the key field must be unique.

The **key field** is the field that you can use with the `in list` operator in queries.

- ♦ The file cannot exceed 25 fields and 2 million rows.
- ♦ The file cannot exceed 150 MB.

Create a Lookup List

- 1 Select **Configuration > Lookup Lists**.
- 2 Select **Add**.
- 3 Drag-and-drop your **CSV file** to the **Lookup Lists** page or select **Browse** to navigate to the file.
- 4 Specify a name for the lookup list.

Once created, you cannot change the name of the lookup list. The name must meet the following requirements:

- ♦ Does not exceed 20 characters
 - ♦ Contains only alphanumeric characters and underscores
 - ♦ Starts with an alpha character
- 5 Specify the **key field**, then either accept the recommended value type or specify a different one.
- The following are possible values:

Value type	Specifies
domain	
float	A number whose radix point can be placed anywhere relative to the significant digits of the number
hostname	Fully qualified domain name
int	Integer value
ipv4	IPv4 address
ipv6	Ipv6 address
mac	MAC address
short text	Text that cannot exceed 1K of space
long text	Text that cannot exceed 4K of space
time	Time stamp
url	A URL address that cannot exceed 4K
username	A string type

- 6 To upload the file as a table in the database, select **Upload**.

Replace a Lookup List

Replacing the contents of a lookup list does not affect queries that use the original lookup list. You cannot change the name of a lookup list. The field names in the replacement file must match the field names in the original file.

- 1 Select **Configuration** > **Lookup Lists**.
- 2 Select the list you want to replace.
- 3 Select **Replace**.
- 4 Select the CSV file you want to use to replace the contents of the existing lookup list.

Delete a Lookup List

- 1 Select **Configuration** > **Lookup Lists**.
- 2 Select the list you want to delete.
- 3 Select the **Trash can** icon.

Use Specific Sets of Fields for Search Results

*You must have the **Create Fieldsets** permission.*

You can specify a **fieldset** that determines a group of search result fields the system displays in the [Events table](#). In the table, each field can provide the ten most and less common values. Multiple searches can share a fieldset, and new searches display a default fieldset that contains the most common event fields. Use the fieldsets window to view and add the customize and system fieldsets, including [lookup lists](#).

- ♦ System: Predefined fieldsets provided by the system.
- ♦ Custom: Customize the default fieldsets and lookup list fields for individual purposes.

New searches display the user's default fieldset. These will remain selected in the fieldsets drop-down even when moving to other search tabs. If you select another fieldset, the popup window closes, displaying the new option. A message will display allowing you to revert the change to the previously selected fieldset.

NOTE: Whenever you replace or update the fieldset, your search becomes out of sync, since the fields shown might differ from the new selection. Rerun the search with the new selection to correct this.

- ♦ [“View and Create Fieldsets” on page 52](#)
- ♦ [“Create a Fieldset” on page 52](#)
- ♦ [“Edit a Fieldset” on page 53](#)
- ♦ [“Delete a Fieldset” on page 53](#)
- ♦ [“Clone a Fieldset” on page 54](#)

View and Create Fieldsets

To access the fieldsets window, from the **Search** page, click the fieldset located at the left of the time range selector. By default, the system displays the name of the last used fieldset. You can also perform the following actions:

- ♦ Filter fieldsets by lists
- ♦ Search fieldsets by name or specific field

You can designate a fieldset as your **preferred default**. The fieldset will only be used for your search results and will not affect other users connecting to the same system.

- 1 From the **Search** page, click the fieldset shown to the left of the time range selector.
- 2 From the fieldsets window, click **Create Fieldsets**.
- 3 To view the complete list of available fieldsets, click the filter icon.
 - ♦ Recently Created Fieldsets
 - ♦ My Fieldsets
 - ♦ Recently Updated Fieldsets
 - ♦ All Fieldsets

Create a Fieldset

- 1 From the **Search** page, click the fieldset name (at the left of the time range selector).
- 2 From the fieldsets window, click **Create Fieldsets**.
- 3 Click **+ Add Fieldset**.
- 4 Select or deselect the options, including lookup fields.
 - 4a Drag and drop any field to the **Selected Fields** column. Otherwise, select **Text Editor** to enter the fields that you need.
 - 4b To locate a specific field, use the search field.

NOTE: The fieldset editor displays the coding-style name for search fields. For more information about which fields to choose or type, see [Appendix A, “Mapping Database Names to their Appropriate Search Fields,”](#) on page 173.

- 5 Specify a name for the new fieldset.
 - 5a Each fieldset should have a unique name.
 - 5b Fieldset names are not case sensitive.
- 6 To save the fieldset as default, select the checkbox at the bottom left corner.

The fieldset is used only for your search results and does not affect other users connecting to the same system.
- 7 Click **Save**.
- 8 (Optional) Select **Apply** to this search to customize the original fieldset without overwriting or saving it.

This new option displays in the custom category as Custom. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

- 9 To execute the query again, click **Search**.

Edit a Fieldset

You can edit custom fieldsets only. You cannot modify system fieldsets, and you can only edit one fieldset at the time.

- 1 From the **Search** page, click the fieldset shown to the left of the time range selector.
- 2 (Conditional) To update the currently selected fieldset, from the fieldsets window, select **Edit Fieldset**.
- 3 (Conditional) To update a different fieldset, click **Create Fieldsets**, and then select the **edit** icon.
- 4 Select or deselect the options, including lookup fields.
 - 4a Drag and drop any field to the Selected Fields column. Otherwise, select **Text Editor** to write the fields you need.
 - 4b To locate a specific field, use the **Search** field.
- 5 Update the fieldset name as needed.
- 6 To save the fieldset as default, select the box at the bottom left corner.

The fieldset is used only for your search results and does not affect other users connecting to the same system.
- 7 Click **Save**.
- 8 (Optional) Select **Apply to this search** to customize the existing fieldset without overwriting or saving it.

This option displays in the custom category as **Custom**. The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporal custom fieldset at a time.

Delete a Fieldset

You can delete a fieldset that you have **created**. If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search. You cannot delete a system fieldset.

- 1 From the **Search** page, click the fieldset shown to the left of the time range selector.
- 2 Select **Create Fieldsets**.
- 3 Select the fieldset name checkbox to delete.
- 4 Select the **delete** icon.
- 5 Select **Yes** to proceed.

Clone a Fieldset

When you clone a fieldset, Search creates a copy of the existing fieldset under the shared fieldsets category. You can update the cloned fieldset and give it a different name.

- 1 From the **Search** page, click the fieldset shown to the left of the time range selector.
- 2 Select **Create Fieldsets**.
- 3 Select the specific fieldset checkbox to copy, and then select **Clone**.

Configure the Time Range

A search query can either have a fixed start and end date, where you cannot [refresh](#) data, or a time range that captures the most recent data. For example, if you choose the predefined **Last 30 minutes** setting, Recon updates data upon re-executing the search based on the most recent 30 minutes. Alternatively, you can create a [dynamic date range](#).

The time range that you specify in the time range selector is inclusive. Search includes the whole second as the end time. For example, if you specify a time range between *2018-01-01 12:00:00* and *2018-01-01 12:59:59*, Search includes all data from *2018-01-01 12:00:00.000* to *2018-01-01 12:59:59.999*, inclusive.

- ♦ [“Specify a Dynamic Date Range” on page 54](#)
- ♦ [“Base the Search on the Timestamp for Events” on page 55](#)
- ♦ [“Understand How Time Zones Affect Search Results” on page 56](#)

Specify a Dynamic Date Range

Search offers a flexible, dynamic setting for the time range where you can enter the desired time stamp without using the calendar to specify days, hours, and minutes. The dynamic date range uses the following syntax:

`<dynamic_time>`

or

`<dynamic_time> [+/- <units>]`

For example, to search for events that have occurred in the last two hours, you can specify `$Now - 2h` for **Start time** and `$Now` for **End time**. To find events that have occurred this week, you can enter `$CurrentWeek` for **Start time** and `$Now` for **End time**.

To enter a dynamic date range:

- 1 When viewing a search or starting a query, select the currently specified time range.
- 2 For the start or end time under **Custom Range**, select **Dynamic**.

- 3 To specify the **dynamic_time**, enter one of the following values:

Value	Represents
\$Now	The current minute
\$Today	Midnight of the current day
\$CurrentWeek	Midnight of the previous Monday (or same as <code>\$Today</code> if today is Monday)
\$CurrentMonth	Midnight on the first day of the current month
\$CurrentYear	Midnight on the first day of the current year

- 4 To specify the **units**, enter one of the following values:

Value	Represents
m (lowercase)	Minutes
h	Hours
d	Days
w	Weeks
M (uppercase)	Months

Base the Search on the Timestamp for Events

Search can display results based on the timestamp associated with each event. The database stores three different timestamps for each event. For peak performance, Search automatically uses the Normalized Event Time setting. However, you can specify any timestamp setting for a search. You can also choose to make the timestamp the [default setting](#).

NOTE: The Date Picker displays this Timestamp setting on when searching for events.

Database Receipt Time

Database Receipt Time (dBRT) represents the time when the database received the event. The database considers this timestamp as the *persisted time* of the event.

Device Receipt Time

Device Receipt Time (DRT) represents the time when the connected device claims the event occurred. This timestamp preserves the original time recorded by the device. However, this timestamp might not be credible in all cases. For example, it is possible that the time settings for the connected device are not configured correctly or the clock on the server that hosts the connected device might gain or lose time, which causes the timestamp to be out of sync with the actual time the event occurred.

Normalized Event Time

Normalized Event Time (NET) represents the best known time for an event. Ideally NET is the time when the connected device reported the event occurred (the [DRT](#)) because the device is the most direct known observer of the event occurrence. However, when the DRT for an event

is not within a credible time range compared to the database's time, NET represents the time when the database received the event (the [dBRT](#)). For example, the time on a connected device was configured incorrectly such that DRT for an event is May 29 1975 when the current date in the database when the database received the event is June 29 2020. The database recognizes that the event's May 29 1795 timestamp for DRT is outside the credible time range. Based on the discrepancy with DRT, the database sets NET to June 29 2020 (same as the dBRT).

By default, the DRT value must be within a boundary of -7 days in the past and +1 days in the future from the dBRT. To configure the boundary criteria, see the *Administrator's Guide for ArcSight Recon*.

Understand How Time Zones Affect Search Results

Searches for events in a time range are based on the [timestamps](#) of matching events and use the time zone of the local browser by default. You might need to account for the time zone offset from UTC and from other time zones, including Daylight Savings Time.

You can configure Search results to adjust the time for events to a [specific time zone](#). For example, it's possible that you might create a search while in a one time zone, then view the search from a different computer set to a different time zone. When this occurs, the [Events Timeline](#) converts the time segments to the specified time zone. If the [Events table](#) includes a time attribute, Search converts the time. However, the aggregation reflects the original time zone. For example, if the Events Timeline has seven bars in the original time zone, the number of bars could increase or decrease to reflect the currently specified time zone.

Configure Preferred Settings for Searches

You can [specify the default settings](#) that you want to apply for new searches. For example, you might want all of your searches to return results from the last 24 hours.



Hunting for Undetected Threats

To help you hunt for undetected threats, the **Reports Portal** includes a set of built-in dashboards and reports. You can [view](#) this content based on the tactics and standards established by MITRE, the Cloud Security Alliance, and OWASP. Additional report and dashboards focus on fundamental security issues, such as monitoring firewalls and malware. For rapid access to your regular dashboards, you can [configure](#) the Reports Portal to display those dashboards by default.

- ♦ [Chapter 5, “Viewing Dashboards and Reports,” on page 59](#)
- ♦ [Chapter 6, “Understanding the MITRE ATT&CK Dashboards and Reports,” on page 63](#)
- ♦ [Chapter 7, “Understanding the Cloud Security Dashboards and Reports,” on page 69](#)
- ♦ [Chapter 8, “Understanding the Foundation Dashboards and Reports,” on page 77](#)
- ♦ [Chapter 9, “Understanding the OWASP Security Dashboards and Reports,” on page 85](#)

5 Viewing Dashboards and Reports

Select **Reports** > **Portal**.

When you view the dashboards and reports, be aware that they are not persistent. Once you leave a report or dashboard, you must regenerate the view when you return to the page. If you choose to open a report in a new browser tab, you can leave that tab open to keep the dashboard or report active while you look at other dashboards or reports.

Many reports and dashboards contain pre-built queries. When you run a report or view a dashboard, it might prompt you to provide values for the run-time parameters. Reports also prompt for the start and end time of the data search.

You access the dashboards and reports from the [Reports Portal](#). In the portal, you can print or export the reports; schedule regular notifications of dashboard results; share reports on social media; and email the dashboard or report to others. You can also [configure](#) the Reports Portal to display specific dashboards by default.

- ♦ [“View a Dashboard” on page 59](#)
- ♦ [“View a Report” on page 60](#)
- ♦ [“Choose Default Dashboards for the Reports Portal” on page 60](#)

View a Dashboard

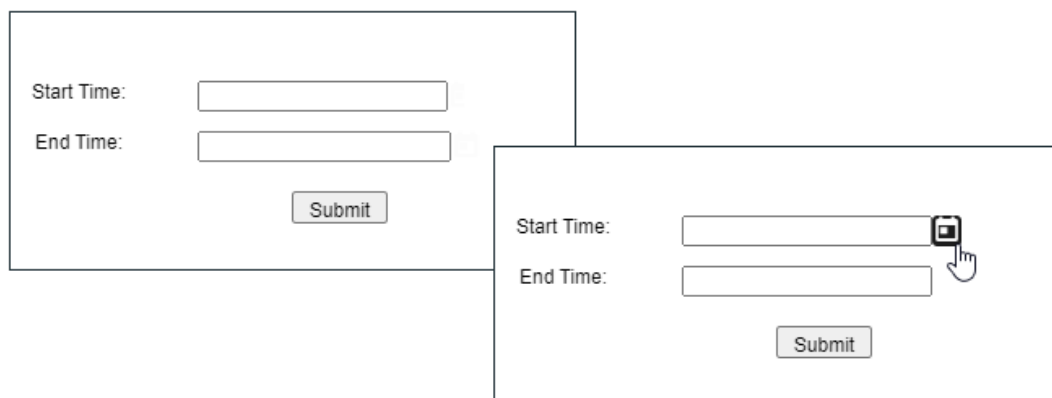
When you open a dashboard, it automatically retrieves data from the last two hours. However, you can modify the time range as needed. You can also configure the settings for the dashboard, then create a bookmark for that configuration.

- 1 Select **Reports** > **Portal** > **Repository** > **Standard Content**.
- 2 Expand the desired category, then select the [dashboard](#) that you want to view.
- 3 (Optional) To change the time range for the report, modify the start or end time parameters.
When you change the time range, the dashboard refreshes the data.

View a Report

When you open a report, you must define the time range for the data you want to view.

- 1 Select **Reports > Portal > Repository > Standard Content**.
- 2 Expand the desired category, then select the **report** that you want to view.
- 3 To change the time range, complete the following steps:
 - 3a To activate the Calendar, point your cursor at the position of the **Calendar** icon to the right of the time selection box.



- 3b Select the **Calendar** icon.
 - 3c Enter the **Start Time** for the report.
 - 3d Enter the **End Time** for the report.
- 4 Select **Submit**.

The report will execute and display when it is complete.
- 5 (Optional) To email the report when it completes, select **Add to Queue**, then define the delivery options.

Choose Default Dashboards for the Reports Portal

The Reports feature allows you to specify the default dashboards that display when you enter the **Reports Portal**. You can choose from any of the content available within the Reports Repository. Alternatively, if you have the *Design Reports* permission, you can create dashboards that you or others might want to include in their default dashboard.

For example, in the Reports Portal, you might want a ready access to dashboards that you use regularly. So you add the **MITRE ATT&CK Overview**, the OWASP **Attacks and Suspicious Activity**, and **Denial of Service Activity** dashboards.

To specify default dashboards:

- 1 Select **Reports > Portal > Portal Dashboards**.
- 2 Specify a name for your default dashboard.
- 3 (Optional) Enter a description for your dashboard portal.

- 4 Select one of the available dashboards.

You can specify only one dashboard at this time. However, once you are in the Reports Portal, you can add more dashboards. Each dashboard appears as a tab in the page.

- 5 (Conditional) To create a dashboard, select **Compose Dashboard**.

- 6 Click **OK**.

- 7 (Conditional) If you chose to create a dashboard, continue adding the items that you want to include. For additional instructions, select **(?)**.

6 Understanding the MITRE ATT&CK Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **MITRE**.

The MITRE ATT&CK dashboards and reports provide you with an immediately recognizable frame of reference, allowing you to view the activity based on content from Enterprise Security Manager for the MITRE ATT&CK matrix and identify possible security gaps. The dashboards and reports also provide you with valuable resources to aid you in your hunt for undetected threats in your enterprise by helping you recognize patterns and trends in the MITRE ATT&CK events.

The dashboards display a visualization based on tactics. In addition to the high-level dashboards, the MITRE ATT&CK reports provide you with detailed information to help you identify security threats.

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. Many companies use MITRE as the go-to source for classifying various types of adversary behaviors. MITRE's periodic table and radial chart enable you to show the linkage between a specific adversary behavior and the subsystem. You can access more detailed information on MITRE tactics and techniques (**MITRE IDs**) on the [MITRE ATT&CK website \(https://attack.mitre.org/\)](https://attack.mitre.org/).

Dashboards	Reports
MITRE ATT&CK Overview Evaluation Techniques and Tactics Summary	MITRE ATT&CK Destination Address Summary MITRE ATT&CK Destination Host Summary MITRE ATT&CK Destination Username Summary MITRE ATT&CK Source Address Summary MITRE ATT&CK Source Hostname Summary MITRE ATT&CK Source Username Summary MITRE ATT&CK Technique Summary

MITRE ATT&CK Dashboards

Content in a MITRE dashboard depends on the widgets that it displays, as well as the dashboard's specified time range.

- ♦ [“MITRE ATT&CK Overview”](#) on page 64
- ♦ [“Evaluation Techniques and Tactics Summary”](#) on page 64

MITRE ATT&CK Overview

The **MITRE ATT&CK Overview** dashboard provides a view of MITRE ATT&CK events forwarded to Recon from ArcSight ESM. This dashboard includes the following charts:

Top 10 Destination Hostnames

Provides a list of the Top 10 destination host names of MITRE ATT&CK events.

Top 10 Source Hostnames

Provides a list of the Top 10 source host names of MITRE ATT&CK events.

MITRE IDs by Destination Hosts

Indicates whether a destination host is involved in one to three MITRE IDs. The size of the solid ovals in the chart are an approximate graphical representation of the count of the MITRE IDs. To get the actual count, move your cursor over the oval.

Source Hosts by MITRE IDs

Indicates whether the same MITRE ID is involved in one to three source host names. The color of the solid ovals in the chart indicate the count for the host name shown in the oval when compared to the legend. To get the actual count, move your cursor over the oval.

Top Destination IPs

Provides the Top 10 destination IP addresses related to a MITRE ID. The donut chart represents the number of times an IP address was the destination of a MITRE ID: the larger the area, the higher the count. The legend is not sorted by count.

Top Source IPs

Provides the Top 10 Source IP addresses related to a MITRE ID. The pie chart is evenly distributed by size among the IP addresses. The count is indicated by the color of the pie piece.

Destination Usernames by MITRE ID

Shows whether one or two destination user names are involved in the same MITRE ID.

MITRE IDs by Source Username

Shows the usernames involved with a MITRE ID (up to 10).

Evaluation Techniques and Tactics Summary

The **Summations of the Evaluation Techniques and Tactics** dashboard shows the total detection count by techniques and tactics. This dashboard includes the following bar charts:

Total Technique by Tactic

Displays the top tactics

Total Techniques by ID

Displays the top technique IDs (up to 30)

Total Technique IDs by MITRE Name

Displays the top MITRE names (up to 20)

Total Techniques IDs by Event Name

Displays the top technique event names (up to 20)

MITRE ATT&CK Reports

Each MITRE ATT&CK report provides a Top 10 summary of different MITRE ATT&CK events. By reviewing these summaries, you might identify a host or user that is the source or target of an attack.

- ♦ [“MITRE ATT&CK Destination Address Summary” on page 65](#)
- ♦ [“MITRE ATT&CK Destination Host Summary” on page 65](#)
- ♦ [“MITRE ATT&CK Destination Username Summary” on page 66](#)
- ♦ [“MITRE ATT&CK Source Address Summary” on page 66](#)
- ♦ [“MITRE ATT&CK Source Hostname Summary” on page 66](#)
- ♦ [“MITRE ATT&CK Source Username Summary” on page 66](#)
- ♦ [“MITRE ATT&CK Technique Summary” on page 67](#)

MITRE ATT&CK Destination Address Summary

The **MITRE ATT&CK Destination Address Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination addresses. In addition to the graph, the report includes a second page that provides the following information about the addresses:

- ♦ Destination Address
- ♦ Destination Username
- ♦ MITRE ID
- ♦ Event Name
- ♦ Count

MITRE ATT&CK Destination Host Summary

The **MITRE ATT&CK Destination Host Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination host names. In addition to the graph, the report includes a second page that provides the following information about the host names:

- ♦ Destination Host Name
- ♦ Destination Username
- ♦ MITRE ID
- ♦ Event Name
- ♦ Count

MITRE ATT&CK Destination Username Summary

The **MITRE ATT&CK Destination Username Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 destination usernames. In addition to the graph, the report includes a second page that provides the following information about the usernames:

- ♦ Destination Username
- ♦ Destination Host Name
- ♦ MITRE ID
- ♦ Event Name
- ♦ Count

MITRE ATT&CK Source Address Summary

The **MITRE ATT&CK Source Address Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source addresses. In addition to the graph, the report includes a second page that provides the following information about the addresses:

- ♦ Source Address
- ♦ Source Username
- ♦ MITRE ID
- ♦ Event Name
- ♦ Count

MITRE ATT&CK Source Hostname Summary

The **MITRE ATT&CK Source Hostname Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source host names. In addition to the graph, the report includes a second page that provides the following information about the host names:

- ♦ Source Hostname
- ♦ Source Username
- ♦ MITRE ID
- ♦ Event Name
- ♦ Count

MITRE ATT&CK Source Username Summary

The **MITRE ATT&CK Source Username Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 source usernames. In addition to the graph, the report includes a second page that provides the following information about the usernames:

- ♦ Source Username
- ♦ Source Hostname
- ♦ MITRE ID

- ♦ Event Name
- ♦ Count

MITRE ATT&CK Technique Summary

The **MITRE ATT&CK Technique Summary** report provides a bar graph of the MITRE ATT&CK events by the Top 10 technique summaries. In addition to the graph, the report includes a second page that provides the following information about the technique summaries:

- ♦ MITRE ID
- ♦ Event Name
- ♦ Destination Username
- ♦ Source Username
- ♦ Count

7 Understanding the Cloud Security Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud**.

Cloud services providers are highly accessible, and the vast amount of data that they host makes them an attractive target for malicious users. To help you assess the security of services in the cloud, we provide dashboards and reports based on the industry-wide standards set by the [Cloud Security Alliance \(CSA\)](https://cloudsecurityalliance.org) (<https://cloudsecurityalliance.org>). This alliance has identified the most significant security threats to the shared, on-demand nature of cloud computing. CSA refers to these issues as the **Treacherous 12**.

Reporting includes the following dashboards and reports, organized by the Treacherous 12 categories:

Category	Dashboards	Reports
Abuse and Nefarious Use of Cloud Services	DoS Originated from EC2 Instances EC2 Instances Communicating with Cryptocurrency Entity EC2 Instances Querying Domains Involved in Phishing Attacks EC2 Machines Involved in Suspicious Communication Email Spam Originated from EC2 Instances Nefarious Activity by an Unauthorized Individual from EC2 Suspicious Activity Reported by Microsoft Azure Trojans or Backdoors Installed on EC2 Instances	<i>n/a</i>
Account Hijacking	Account Hijacking Vulnerabilities Man in the Middle Attacks Phishing Attacks Principal Invoked an API Commonly used to Discover Information Associated with AWS Account	Broken Authentication and Session Management
Advanced Persistent Threats	Trojans or Backdoors installed on EC2 Instances	<i>n/a</i>
Data Breaches	All Information Leakage Events Information Disclosure Vulnerabilities Organizational Information Leakage Personal Information Leakage	<i>n/a</i>

Category	Dashboards	Reports
Data Loss	Amazon AWS Deletion Events	Amazon S3 Bucket Deletion Events Amazon VPC Deletion Events
Denial of Service	DoS Activity	<i>n/a</i>
Insecure Interfaces and APIs	<i>n/a</i>	Vulnerabilities on Interfaces and API
Insufficient Due Diligence	<i>n/a</i>	EC2 Machines Behavior Deviates from the Established Baseline Failed Technical Compliance Events
Insufficient Identity Credential and Access Management	<i>n/a</i>	AWS Account Password Policy Was Weakened Invalid or Expired Certificate Unsecured Password Events
Malicious Insiders	<i>n/a</i>	Nefarious Activity by an Unauthorized Individual
System Vulnerabilities	Vulnerability Overview	Cloud Related Vulnerabilities Critical Vulnerabilities Heartbleed Vulnerabilities Kernel Vulnerabilities Overflow Vulnerabilities Security Patch Missing Shellshock Vulnerabilities Spectre and Meltdown Vulnerabilities Vulnerabilities by Host
Vulnerabilities on Shared Technologies	<i>n/a</i>	Vulnerabilities on Shared Technologies

The cloud-based security dashboards and reports provide a view of events occurring in Amazon Web Service (AWS) and Azure, forwarded to Recon from ArcSight ESM. Content in a dashboard depends on the widgets that it displays, as well as the dashboard's specified time range. For example, some widgets summarize events by resource names and profile IDs, as well as by the event's severity.

Abuse and Nefarious Use of Cloud Services – Dashboards

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Malicious users can exploit poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups, which expose cloud computing models such as IaaS, PaaS, and SaaS. You might experience denial of service attacks, email spam and phishing campaigns, and brute-force computing attacks, or malicious individuals spoofing identities.

Some charts display data reported by Amazon GuardDuty, which is a threat detection service that continuously watches for malicious activity and unauthorized behavior.

To search for potential threats, use the following dashboards:

DoS Originated from EC2 Instances

Helps you identify denial of services activities that arise from EC2 (AWS Elastic Compute Cloud service) instances. The charts and table show events summarized by their Amazon resource name, severity, and GuardDuty.

EC2 Instances Communicating with Cryptocurrency Entity

Displays EC2 instances that communicates with cryptocurrency IP addresses or domains.

EC2 Instances Querying Domains Involved in Phishing Attacks

Lists the EC2 instances in which querying domains are involved in phishing attacks.

EC2 Machines Involved in Suspicious Communication

Lists the EC2 machines that are involved in suspicious communication.

Email Spam Originated from EC2 Instances

Identifies email spam that originates from EC2 instances.

Nefarious Activity by an Unauthorized Individual from EC2

Displays events that Amazon GuardDuty reports as nefarious activity by an unauthorized individual from EC2 machines. Amazon GuardDuty a threat detection service that continuously watches for malicious activity and unauthorized behavior.

Suspicious Activity Reported by Microsoft Azure

Lists suspicious activity reported by Microsoft Azure.

Trojans or Backdoors Installed on EC2 Instances

Lists backdoors or trojans discovered on EC2 machines.

Account Hijacking – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

CSA identifies the hijacking of accounts and services as an ongoing, top threat. Malicious users might hijack accounts by phishing, fraud, and exploiting software vulnerabilities. In the cloud, the hijackers can eavesdrop on organizational activities, manipulate data, and redirect your clients.

To search for potential threats, use the following dashboards and report:

Account Hijacking Vulnerabilities

Provides charts of the top 10 vulnerabilities and the number of vulnerabilities over time. This dashboard also includes a table of the vulnerabilities, so you can review the reporting vendor or device, agent severity, asset, and the asset's zone.

Man in the Middle Attacks

Provides charts that show man in the middle events by time, source address, destination address, source MAC address, and destination MAC address.

Phishing Attacks

Provides charts that show the phishing attacks against the organizations.

Principal Invoked an API Commonly used to Discover Information Associated with AWS account

Provides charts that show the principals invoked by an API commonly used to discover information associated with AWS accounts.

Broken Authentication and Session Management

Lists the events that might be associated with broken authentication (possibly hijacked credentials) and session management issues reported by vulnerability scanners in the organization.

Advanced Persistent Threats – Dashboard

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Advanced Persistent Threats (APTs) are a parasitical form of cyberattack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. This category provides the **Trojans or Backdoors Installed on EC2 Instances** dashboard, which provides charts showing backdoors or trojans discovered on EC2 (AWS Elastic Compute Cloud service) machines. This dashboard also is available within the [Abuse and Nefarious Use of Cloud Services – Dashboards](#) category.

Data Breaches – Dashboards

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

While the risk of a data breach is not unique to the cloud, the CSA ranks it as a top concern for cloud customers. Sometimes the breach is the prime motivation of malicious users. However, breaches also result from mistakes made by individuals within the organization or poor security practices and software vulnerabilities.

To search for potential threats, use the following dashboards:

All Information Leakage Events

Provides charts and a table that show the leakage events in the organization, including the top reported events, destination users, and assets.

Information Disclosure Vulnerabilities

Provides charts and a table that show the disclosure vulnerabilities reported in the organization over time and by agent severity. You can also see the top 20 hosts, IP addresses, and signature ID events.

Organizational Information Leakage

Provides charts and a table that show the leakage of organizational information. You can view the top 20 leakage events and signature IDs, as well as leakage over time and agent severity.

Personal Information Leakage

Provides charts and a table that show the leakage of personal information. You can view the top reported, top 10 destination and source users, and leakage over time.

Data Loss – Dashboard and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

No organization wants to lose data, particularly to malicious individuals who might use the information in an adverse manner. Unfortunately, data stored in the cloud can also be deleted accidentally or as a result of a catastrophe.

To assess the potential for data loss, use the following reports:

Amazon S3 Bucket Deletion Events

Lists the deletion events that occur in Amazon S3 Buckets.

Amazon VPC Deletion Events

Lists the deletion events that occur in Amazon VPC.

This category includes the **Amazon AWS Deletion Events** dashboard, which provides charts and a table listing the number of deletion events by operations, day, source address, and source user.

Denial of Service – Dashboard

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Denial-of-service (DoS) attacks deliberately attempt to prevent users from accessing services, data, and applications. Use the **DoS Activity** dashboard to watch for potential service interruptions. You can view the top source and destination addresses, as well as events by day.

This dashboard also is available in the [Network Monitoring](#) category of the [Foundation](#) reports.

Insecure Interfaces and APIs – Report

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Users interact with cloud computing services through user interfaces (UIs) and application program interfaces (APIs), and the value-added services built on these services. APIs and UIs are generally the most exposed part of a system, perhaps the only asset with an IP address available outside the trusted organizational boundary. These assets will be the target of heavy attack. Use the **Vulnerabilities on Interfaces and API** report to identify the vulnerabilities found in your cloud-based interfaces and APIs.

Insufficient Due Diligence – Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

The CSA states that it is essential to develop a good roadmap and checklist for due diligence when evaluating technologies and CSPs. Organizations should perform due diligence to mitigate the myriad risks associated with providing cloud services. To identify areas with insufficient due diligence, use the following reports:

EC2 Machines Behavior Deviates from the Established Baseline

Details how the behavior of EC2 (AWS Elastic Compute Cloud) machines deviates from the established baseline.

Failed Technical Compliance Events

Lists the failed technical compliance events.

Insufficient Identity Credential and Access Management – Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Malicious users can infiltrate and cause data breaches based on poor authentication methods and weak password policies. Use the following reports to watch for threats due to insufficient identity credentials and access management:

AWS Account Password Policy Was Weakened

Lists events associated with weakened AWS account password policy.

Invalid or Expired Certificate

Lists events associated with invalid or expired certificates.

Unsecured Password Events

Lists events associated with unsecured passwords.

Malicious Insiders – Report

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **CSA** > **The Treacherous 12**.

Individuals within an organization, such as system administrators or disgruntled colleagues, might access sensitive information for malicious intent. Most organizations use controls to limit risk from malicious insiders, such as controlling encryption keys and monitoring or auditing the activities of specific users.

The **Nefarious Activity by an Unauthorized Individual** report lists events that Amazon GuardDuty reports as nefarious activity by an unauthorized individual from EC2 (AWS Elastic Compute Cloud) machines. Amazon GuardDuty is a threat detection service that continuously watches for malicious activity and unauthorized behavior.

System Vulnerabilities – Dashboard and Reports

Select > **Reports** > **Portal** > **Repository** > **Standard Content** > **Cloud** > **System Vulnerabilities**.

Most computer systems have programs, services, and operating systems that are vulnerable to exploitation. According to the CSA, vulnerabilities within the components of the operating system – kernel, system libraries and application tools – put the security of all services and data at significant risk.

To mitigate the risk to your systems, use the following reports and dashboard:

Cloud Related Vulnerabilities

Lists all events associated with vulnerabilities known to affect AWS and Azure.

Critical Vulnerabilities

Lists all events that have a *High* or *Very High* severity, based on CVE and CVSS data.

Heartbleed Vulnerabilities

Lists all events associated with the heartbleed bug, which is a system vulnerability in the OpenSSL cryptographic software library. This weakness allows malicious users to steal the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. A Heartbleed attack works by tricking servers into leaking information stored in their memory. Attackers can also get access to a server's private encryption key, allowing the attacker to unscramble any private messages sent to the server and even impersonate the server.

Kernel Vulnerabilities

Lists all events associated with kernel vulnerabilities. For example, the vulnerability in the Linux Kernel `netfilter/xt_TCPMSS`, which could allow remote hackers to carry out a denial of service attack.

Overflow Vulnerabilities

Lists all events associated with buffer overflows. When a buffer receives more data than it can handle, the data can overflow to other storage locations. Overflows can cause system crashes or create an exploitable vulnerability.

Security Patch Missing

Reports the hosts that do not have the security patches needed to resolve known vulnerabilities.

ShellShock Vulnerabilities

Reports the hosts vulnerable to a ShellShock attack. In a ShellShock attack, the Unix shell Bash could execute arbitrary commands and allow unauthorized access to services, such as web servers, that use Bash to process requests.

Spectre and Meltdown Vulnerabilities

Reports the hosts vulnerable to Meltdown and Spectre attacks, which exploit critical vulnerabilities in modern processors. Meltdown breaks the fundamental isolation between user applications and the operating system, allowing a program to access the memory and data of other programs and the operating system. Spectre attacks break the isolation between applications, allowing programs to leak information to each other. These exploitations do not leave any traces in traditional log files.

Vulnerability Overview

Provides a dashboard view of the vulnerabilities found in the organization.

Vulnerabilities by Host

Lists all vulnerabilities detected on the specified hosts.

Vulnerabilities on Shared Technologies

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Cloud](#) > [CSA](#) > [The Treacherous 12](#).

Some technologies that form the infrastructure for the cloud-based services started as on-premises capabilities, and thus might not have been designed to share its resources in multi-tenancy or multi-customer environments. For example, an application might not have initially been expected to support multi-factor authentication or a its database designed to partition data by tenant.

The **Vulnerabilities on Shared Technologies** report provides you insight into the vulnerable technologies that a malicious user might exploit.

8 Understanding the Foundation Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

Reporting includes the following dashboards and reports, organized by the following foundational categories:

Category	Dashboards	Reports
Entity Monitoring	Account Management Overview Failed Logins Overview Successful Login Overview	All Logins by Hostname Failed Logins Summary Login Activity by User
Event Overview	Least Common Events Most Common Events Most Common Events by Severity Reporting Devices	<i>n/a</i>
Host Monitoring	<i>n/a</i>	Anti-virus Activity Audit Log Cleared Events Failed Anti-virus Updates Summary Operating System Errors and Warnings Services Shutdown Services Started
Malware Monitoring	Malware Overview	Reported Malware by Host Worm Infected Systems
Network Monitoring	Attacks and Suspicious Activity Overview DGA Overview DoS Activity Email Attacks IDS Events Man in the Middle Attacks Reconnaissance Activity Traffic Anomaly Overview VPN Activities Overview	Exploit Attempts Detected by IDS Network Device Configuration Changes
Perimeter Monitoring	Firewall Blocked Events Firewall Traffic Overview	Firewall Configuration Changes Firewall Blocked Traffic by Destination Address

Category	Dashboards	Reports
Vulnerability Monitoring	<i>n/a</i>	High Risk Vulnerabilities by Host SSL Vulnerabilities Vulnerability Summary by Host XSRF Vulnerabilities XSS Vulnerabilities

Entity Monitoring – Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

To prevent brute force attacks or denial-of-service attacks, you could track login activities in your environment. A malicious user might attempt to guess another user's password by repeatedly attempting to log in to the same account. You can track this behavior by observing failed login attempts. You might also watch for users who attempt to log in to multiple devices and hosts. Malicious users might also create, modify, and delete accounts to gain unauthorized access or let them execute harmful code.

To monitor account activity, use the following dashboards and reports:

Account Management Overview

Provides charts and a table to help you identify users who are creating and deleting the most accounts. You also can track which hosts have had the largest number of accounts modified or deleted.

All Logins by Hostname

Reports the number of login attempts over time, including the outcome, for the specified hosts. You must specify one IP address.

Failed Logins Overview

Provides an overview, in charts and a table, of the hosts and users with the highest number of failed logins. You can also view the number of failed logins over time, by reporting device, or source address.

Failed Logins Summary

Reports the number of failed logins over time. The table includes the user, source address, target host, and number of failed attempts.

Login Activity by User

Reports the number of times that the specified users have attempted to log in to a host. The table indicates whether the attempt is successful.

You must specify one user by `Destination UserName`.

Successful Login Overview

Provides an overview, in charts and a table, of users with the highest number of successful logins. You can review the relationship between the users and the hosts to which they successfully log in.

Events Overview – Dashboards

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

To identify threats in your environment, you might want to have an overview of the events that occur the most often or affect the most devices and hosts. You could also watch for events that rarely occur to check for unusual activity.

To monitor event activity, use the following dashboards:

Least Common Events

Provides charts and a table to help you identify the events that have the fewest reported occurrences. You can view the results by vendor, such as Amazon, or product, such as Microsoft Windows.

Most Common Events

Provides charts and a table to help you identify the common events that affect your environment by vendor, such as Amazon, or product, such as Microsoft Windows.

Most Common Events by Severity

Provides a table to help you track the events by count and severity.

Reporting Devices

Provides charts and a table to help you identify the hosts and devices with the most reported security events. You can view charts summarizing the most common severity of the events; top 20 events by vendor such as Microsoft or McAfee; top 20 events types of events, such as stopped services, and the top 20 events by class ID, such as a CVE.

Hosts Monitoring - Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

In general, you should consistently monitor host-based events that indicate unauthorized activities. For example, a malicious user or program might start and stop host services and anti-virus programs. Additionally, they might clear the audit log to hide their actions on a host.

To monitor unusual activity that affects hosts, use the following reports:

Anti-virus Activity

Reports the volume of activity by reporting anti-virus service. The table provides results by event name, count, affected host, and outcome.

Anti-virus Stopped or Paused

Reports the top IP addresses where an anti-virus service has been stopped or paused. The table provides results by host, service name, and number of events.

Audit Log Cleared

Reports the number of times that the audit log has been cleared by user, host, and date.

Failed Anti-virus Updates Summary

Reports the number of failures in updating anti-virus software by date and host.

Operating Systems Errors and Warnings

Reports the top system errors and warnings by host. You could identify issues associated with specific errors or warnings, such as privileged objects and users, password changes, and login failures. Alternatively, you could sort the table by the reported hosts to review the types of issues affecting each host.

Services Shutdown

Reports the top 10 services that have been shut down in your environment. The table provides a summary of all services, including the associated hosts.

Services Started

Reports the top 10 services that have been started in your environment. The table provides a summary of all services started, including the associated hosts.

Malware Monitoring – Dashboard and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

Malware, or malicious software, represents all the variations of programs designed to damage computers, servers, clients, devices, applications, and networks. To monitor malware activity, use the following dashboard and reports:

Malware Overview

Provides charts and a table to help you identify the malware affecting your enterprise and the top 10 infected hosts. You can also view the malware events reported over time.

Reported Malware by Host

Lists the malware found on the specified hosts.

You must specify one host.

Worm Infected Systems

Lists the hosts infected by worms, and provides a chart that shows the malware by count found in your enterprise.

Network Monitoring – Dashboards and Report

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Foundation**.

The traffic exchanged between devices and servers tells you a lot about your network. By monitoring network traffic, you can identify cyber attacks and network events that could affect your enterprise. For example, malicious users might find a way to intercept communications to generate a man-in-the-middle attack or change the configuration of devices to gain unauthorized access. In both cases, the attack is the beginning of further intrusions. Also, a system infected by malware can be instructed generate a large volume of domains, thus causing increased traffic.

To monitor network activity, use the following dashboards and reports:

Attacks and Suspicious Activity Overview

Provides charts and a table to help you identify the top attackers, targets, and events over time.

This dashboard also is available in the [Insufficient Logging and Monitoring](#) category of the **OWASP** reports.

DGA Overview

Provides charts and a table to help you watch for domain generation algorithms (DGAs). You can identify the IP addresses generating the most DGA domains or the unique domains that the largest number of hosts attempt to connect with. You can also check for the hosts that are transmitting the largest amount of data.

DoS Activity

Provides charts and a table for you to identify [denial-of-service](#) events. You can view the number of events per day, as well as the top source and destination addresses.

This dashboard also is available in the [Denial of Service](#) category of the **Cloud** reports.

Email Attacks

Provides charts and a table that describe the email attacks detected in your enterprise. You can view the top events or target users, as well as the destination and source addresses.

Exploit Attempts Detected by IDS

Shows the top 10 exploit attempts reported by the intrusion detection systems (IDS) in your enterprise. In the table, you can sort the events by count or severity.

IDS Events

Provides a chart and table showing all events reported by the IDSs in your enterprise.

Man in the Middle Attacks

Provides charts and a table to help you catch potential man-in-the-middle (MitM) attacks. You can view events over time, by source and destination address including MAC addresses, and the top MitM events.

During a MitM attack, the malicious user intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two.

Network Device Configuration Changes

Reports the top 10 devices whose configurations have changed, as well as the top 10 events causing configuration changes.

Reconnaissance Activity

Provides charts and a table to help you watch for active reconnaissance attacks. You can view identify the top sources of recon activity, as well as the primary destinations for these attacks. Review the pie charts to identify the main types of events and affected zones.

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. Malicious users might use tools like ping or traceroute to perform recon through automated scanning or manual testing.

Traffic Anomaly Overview

Provides charts to help you identify anomalies in network traffic. You can view the top source and destination address, events, and activity over time.

VPN Activities Overview

Provides charts and a table for you to monitor VPN activity, such as the top users who access the VPN. You can view the VPN activities per day, as well as review the top source and destination addresses.

Perimeter Monitoring – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

The perimeters of an enterprise's network handle a great deal of traffic, causing system administrators to face an ever-increasing need to allow fast, efficient flow of traffic while also keeping the network secure. If you pro-actively monitor the firewalls in your enterprise, you can identify problems at an early stage and prevent network attacks. Malicious users often exploit loopholes in your firewall rules, particularly any old or unused rules. Network traffic also can be vulnerable to unencrypted data.

To monitor your network's perimeter, use the following dashboards and reports:

Firewall Blocked Events

Provides charts and a table for you to monitor the events that your firewalls have blocked, such as the bytes in and out for all blocked events. You can view the top events blocked per device, application protocol, source address, or destination address.

Firewall Blocked Traffic by Destination Address

Lists the top 10 firewall traffic events that have been blocked from reaching the specified hosts. You must specify one IP address.

Firewall Configuration Changes

Lists the top 10 changes to the firewall configuration by host.

Firewall Traffic Overview

Provides charts and a table for you to monitor traffic through your firewalls, such as the bytes in and out by accepted and denied traffic. You can view the top reporting devices and destination addresses, as well as the outcomes of port usage over time. The table lists the Port, transport protocol, application protocol, and number of events reported by firewalls.

Vulnerability Monitoring – Dashboard and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [Foundation](#).

Many of the components within a web application, such as the libraries and modules, run with the same privileges as the application itself. Applications and APIs using components with known vulnerabilities can undermine application defenses and enable various attacks and impacts. For example, malicious users can exploit a known in SSL with the [Heartbleed Bug](#). Web site and web applications can be vulnerable to [cross-site scripting \(XSS\)](#) and cross-site request forgery (XSRF) attacks. In an XSRF attack, also known as a one-click attack or session riding, a malicious user submits unauthorized commands to a web application from a user account that the application trusts.

High-risk vulnerabilities represent those that are relatively easy for attackers to exploit and gain control over system components. Many high-risk vulnerabilities can temporarily or permanently disrupt enterprise operations.

To check whether your enterprise has vulnerabilities, use the following dashboard and reports:

High Risk Vulnerabilities by Host

Lists all high-risk vulnerabilities found on the specified hosts.

You must specify one host by `Destination Host`.

SSL Vulnerabilities

Lists the hosts reported to have the most SSL vulnerabilities.

This report also is available in the [Using Components with Known Vulnerabilities](#) category of the **OWASP** reports.

Vulnerability Overview

Provides charts and a table to help you track the vulnerabilities reported in your enterprise.

Vulnerabilities by Host

Lists all vulnerabilities found on the specified hosts.

You must specify one IP address.

XSRF Vulnerabilities

Lists the top 10 hosts that are vulnerable to a cross-site request forgery (XSRF or CSRF) attack.

XSS Vulnerabilities

Lists the top 10 hosts that are vulnerable to [cross-site scripting \(XSS\)](#) attacks.

9 Understanding the OWASP Security Dashboards and Reports

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP**.

We provide dashboards and reports based on the industry-wide standards set by the [Open Web Application Security Project®](https://owasp.org) (<https://owasp.org>). OWASP is a nonprofit foundation that works to improve the security of software. The organization has established a list of the Top 10 security risks to web applications, focusing on the most critical threats to the shared, on-demand nature of web-based applications.

Reporting includes the following dashboards and reports, organized according to **OWASP's Top 10 risk** categories:

Category	Dashboards	Reports
Broken Access Control	<i>n/a</i>	Broken Access Control
Broken Authentication	<i>n/a</i>	Broken Authentication and Session Management
Cross-site Scripting	Cross Site Scripting	XSS Vulnerabilities
Injections	Injection Vulnerabilities Overview	Command Injections on HTTP Request Injection Vulnerabilities SQL Injection
Insecure Deserialization	Deserialization Flaws Overview	Deserialization Flaws
Insufficient Logging and Monitoring	Attacks and Suspicious Activity Failed Logins Overview Login Activity Overview Operating System Errors and Warnings Security Log is Full	All Logins by Hostname Audit Log Cleared Failed Logins Summary
Security Misconfiguration	Misconfiguration Events Overview Missing Security Patches Overview	Security Patch Missing
Sensitive Data Exposure	Information Leaks Overview	Organizational Records Information Leaks Personal Information Leaks
Using Components with Known Vulnerabilities	SSH Vulnerabilities Overview Vulnerability Overview	SSH Vulnerabilities Summary SSL Vulnerabilities

Category	Dashboards	Reports
XML External Entities	XML Vulnerabilities Overview	XML Vulnerabilities

Broken Access Control

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 5 - Broken Access Control](#).

Some enterprises fail to enforce access controls that restrict what authenticated users are allowed to do. By exploiting vulnerabilities in access controls, a malicious user might retrieve sensitive files, gain access other user's accounts, change access rights, and misuse data.

The **Broken Access Control** report lists vulnerable hosts by severity over time.

Broken Authentication

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 2 - Broken Authentication](#).

Some enterprises fail to enable or mis-configure the authentication and session management functions of applications and web sites. When this occurs, a malicious user could compromise passwords, keys, and session tokens.

Use the **Broken Authentication and Session Management** report to identify hosts vulnerable to malicious users. This report also is available in the [Account Hijacking](#) category of the **Cloud** reports.

Cross-site Scripting

Select > [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 7 - Cross-Site Scripting](#).

Vulnerabilities associated with **cross-site scripting (XSS)** enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The scripts might hijack user sessions, deface web sites, or redirect users to harmful sites. A web application or web page becomes vulnerable when it includes untrusted data; data without proper validation or escaping; or data supplied by users through an API that can create HTML or Java-script. XSS attacks tend to occur in forums, message boards, and web pages that allow comments. Malicious users can execute XSS attacks in VPScript, ActiveX, Flash, and CSS. However, this type of injection attack most commonly occurs in Java Script.

To identify XSS vulnerabilities in your environment, use the following report and dashboard:

Cross Site Scripting

Lists events associated with XSS vulnerabilities.

XSS Vulnerabilities

Provides charts and a table so you can review potential XSS vulnerabilities in your environment by vulnerability type or the top vulnerable hosts.

To get a list of the top 10 hosts vulnerable to cross-site scripting attacks, run the [XSS Vulnerabilities](#) report.

Injections

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 1 - Injections](#).

Injection vulnerabilities, or flaws, allow malicious users to inject code in other systems, especially interpreters, by using vulnerable applications. For example, in a SQL, NoSQL, OS or LDAP injection attack, someone sends untrusted data to an interpreter as part of a command or query to trick the interpreter into executing hostile commands or accessing data without appropriate authorization. Usually, these flaws result from insufficient validation of data input or the failure to filter or sanitize the input.

To check for injection vulnerabilities, use the following reports and dashboard:

Command Injections on HTTP Request

Lists the highest number of events associated with command injections in an HTTP request, by the requested URL. This report includes a chart to help you identify the relationship between the IP addresses of the attacker and the target.

In a command injection attack that exploits an HTTP request, malicious users execute arbitrary commands on the host operating system via a vulnerable application. For example, the web application passes unsafe data supplied by the user to a system shell.

Injection Vulnerabilities

Lists the hosts with the most injection vulnerabilities over time.

Injection Vulnerabilities Overview

Provides charts and a table to help you identify the systems affected by injection vulnerabilities, as well as view the top reported vulnerabilities by agent severity, risk, and over time.

SQL Injection

Lists the systems with the highest number of SQL injection vulnerabilities.

In a SQL injection attack, a malicious user can interfere with the queries that an application makes to its database. The user could view delete, or modify data not usually available for retrieval. A malicious user could also use SQL injections to start a denial-of-service attack or compromise other services, servers, or infrastructure.

Insecure Deserialization – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 8 - Insecure Deserialization](#).

Untrusted, or insecure, deserialization allows malicious users to use untrusted data to abuse the logic of an application, initiate a denial-of-service or injection attacks, or execute harmful code when the data is deserialized. The user could even replace a serialized object with objects of a different class. Deserialization is a common process where the web site or application takes data from a file, stream, or network and rebuilds it into an object. The serialized objects might be used in JSON, XML, or YAML.

To check for deserialization vulnerabilities, use the following report and dashboard:

Deserialization Flaws

Lists the hosts with most deserialization flaws.

Deserialization Flaws Overview

Provides charts and a table to help you identify the top hosts, deserialization flaws, and flaws found over time. You can view the flaws by agent severity and risk indicator.

Insufficient Logging and Monitoring – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 10 - Insufficient Logging and Monitoring](#).

According to OWASP, insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows malicious users to further attack systems; maintain persistence; pivot to more systems; and tamper, extract, or destroy data. Most major incidents start with an exploitation of the vulnerabilities in logging and monitoring. Yet, most organizations fail to discover the breach until several months have passed.

To help you detect potential breaches as soon as possible, use the following reports and dashboards:

All Logins by Hostname

Lists all logins that have occurred on the specified host.

Attacks and Suspicious Activities Overview

Provides charts and a table to help you identify the top attackers, targets, and events over time.

This dashboard also is available in the [Network Monitoring](#) category of the [Foundation](#) reports.

Audit Log Cleared

Lists all the Audit Clear events that have occurred in the organization.

Failed Logins Overview

Provides charts and a table showing failed logins by time, users, hosts, reporting devices, and attacker address.

Failed Logins Summary

Lists the failed login events that have occurred in your environment.

Login Activity Overview

Provides charts and a table showing the outcome of login activity, including successful logins. You can view activity by machine or user, as well as a chart showing the relationship between users and systems to which they log in.

Operating System Errors and Warnings

Provides charts and a table that report the operating systems errors and warnings in the organization.

Security Log is Full

Provides charts and a table to help you identify the hosts where the security log is full.

Security Misconfiguration

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 6 - Security Misconfiguration](#).

In general, the most common vulnerability in your environment is mis-configured operating systems, frameworks, libraries, and applications. Mis-configurations include missing security patches or updates, incomplete or ad hoc configurations, use of insecure default configurations, poorly configured HTTP headers, and error messages that contain sensitive information.

To identify systems that need reconfiguration, use the following dashboards and report:

Misconfiguration Events Overview

Provides an overview of the mis-configured events reported in your environment. The charts show the top mis-configured systems, the top misconfiguration events, an indicator of the risk associated with the reported misconfiguration events, events by agent severity, and misconfiguration events over time. The table provides additional information, such as the associated vulnerability.

Missing Security Patches Overview

Provides charts and a table to help you identify the top machines that fail to have all relevant security patches, as well as the security patches most reported as not having been applied. You can review the missing patch reports over time, by agent severity, and by risk indicator.

Security Patch Missing

Lists the security patches that have not been applied, as reported by vulnerability scanners in your environment.

Sensitive Data Exposure

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 3 - Sensitive Data Exposure](#).

Most enterprises store sensitive data that needs to be protected, such as personal information, customer and organizational financial data, healthcare records, or intellectual property. Web applications and APIs might inadvertently expose sensitive data by not having enough protections such as encryption at rest or in transit, or when exchanging data with the browser. Malicious users could use the data for credit card fraud, identity theft, and other crimes.

To identify potential exposure of sensitive data, use the following dashboard and reports:

Information Leaks Overview

Provides charts and a table to help you identify the most reported systems, types of leaks, and leakage events that occur over time. You can identify the top reported users and view leaks by category.

Organizational Records Information Leaks

Lists the top leakage events that affect organizational records.

Personal Information Leaks

Lists the top leakage events that affect personal records by Destination UserName.

Using Components with Known Vulnerabilities – Dashboards and Reports

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 9 - Using Components with Known Vulnerabilities](#).

Many of the components within a web application, such as the libraries and modules, run with the same privileges as the application itself. Applications and APIs using components with known vulnerabilities can undermine application defenses and enable various attacks and impacts. Malicious users can exploit vulnerabilities in SSH and SSL. For example, the [Heartbleed Bug](#) is a known SSL vulnerability. Your enterprise might have large numbers of SSH keys because end users can create new SSH keys (credentials) or even duplicate them without oversight, unlike certificates or passwords. A malicious user can gain long-term access to your resources by taking advantage of SSH keys that have been left unaccounted for.

To check whether components can be exploited, use the following dashboards and reports:

SSH Vulnerabilities Overview

Provides charts and a table that show hosts with the most SSH vulnerabilities and the most reported vulnerabilities. You can review these vulnerabilities over time, by agent severity, and by risk indicator.

SSH Vulnerabilities Summary

Lists the hosts reported to have the most SSH vulnerabilities.

SSL Vulnerabilities

Lists the hosts reported to have the most SSL vulnerabilities.

This report also is available in the [Vulnerability Monitoring](#) category of the [Foundation](#) reports.

Vulnerability Overview

Provides charts and a table that show the top signature IDs for the anti-virus programs that have failed to update, as well as the hosts most likely to be vulnerable. You can review these vulnerabilities over time and by agent severity.

XML External Entities

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [OWASP](#) > [A 4 - XML External Entities](#).

Older or mis-configured XML processors use XML documents to evaluate external entity references, and can inadvertently process harmful XML input. Malicious users use the XML processor's to reveal internal content such as files, file shares, and port scans, as well as execute remote code and denial-of-service attacks.

To watch for XML external entity attacks, use the following report and dashboard.

XML Vulnerabilities

Lists the hosts with the most XML vulnerabilities.

XML Vulnerabilities Overview

Provides charts and a table to help you identify the systems with the most XML vulnerabilities as well as the most reported vulnerabilities. You can review the vulnerabilities by severity and risk indicator.



Analyzing Anomalous Data with Outlier Analytics

Select **Insights** > **Outliers**.

To help you identify anomalous behavior, the **Outlier Analytics** feature allows you to compare incoming *EventCount*, *BytesIn*, and *BytesOut* values to typical values for your environment. The *EventCount*, *BytesIn* and *BytesOut* values are aggregations over certain time periods for each host/IP address. Outlier Analytics can create and persist a baseline of host behavior. To derive outliers, you compare this baseline with aggregations over new time periods. Basically, the lower the anomaly score, the more likely the event is anomalous.

The analytics process allows you to [define and build a model](#) that identifies typical behavior for your environment, and then start a [scoring process](#) that evaluates incoming events against the model. The scoring process assigns a score that indicates the degree to which the incoming data varies from the typical behavior. Outlier Analytics [displays the results](#) of the scoring process in a table that shows the top anomalous hosts. From the table, you can generate charts that provide additional information about the anomaly.

The model specifies a subset of data from the [Events table](#) that represents typical behavior on your network. When you define the model, you can specify criteria that identify which device behaviors you want to model. For example, you might want to look for anomalous values in events that you receive from a specific device vendor or in systems on a specific subnet.

- ♦ [Chapter 10, “Generating Models to View Anomalous Data,” on page 95](#)
- ♦ [Chapter 11, “Viewing Anomalous Data in a Model,” on page 99](#)

10 Generating Models to View Anomalous Data

You must have the **Manage Outlier Models and Scoring** permissions to define and build models.

The model for Outlier Analytics defines typical *EventCount*, *BytesIn*, and *BytesOut* behavior for a set of IP addresses over a specified date range. You can define the criteria that identify which device behaviors you want to model. If you want a different model, you must define and build a new one.

- ♦ [“Considerations for Generating Models” on page 95](#)
- ♦ [“Defining and Building a Model” on page 96](#)
- ♦ [“Scoring a Model” on page 96](#)
- ♦ [“Deleting a Model” on page 97](#)

Considerations for Generating Models

Before defining and building a model, review the following considerations:

- ♦ You can create and delete models, but you cannot modify them.
- ♦ You can define as many models as you want, but you can only build one model at a time.
- ♦ When you define the model, you should set the date range wide enough (more than 168 hours) so that the model includes a variety of device behaviors, including cyclical patterns.
- ♦ Because the scoring algorithm is based on peer group analysis, Micro Focus recommends that you include similar devices in a model, based on activity. For example, you might want to create separate models for scoring endpoints, scoring DNS servers, and scoring databases.
- ♦ Each model definition applies a filter where `Source Address != NULL`.
- ♦ When you build a model, Outlier Analytics adds a [lookup list](#) of the same name to **Configuration > Lookup Lists**. You cannot view or edit this list. When you delete the model, the lookup list also gets deleted.
- ♦ The auto-complete functionality is temporarily unavailable in search input. The following columns are available for outliers filtering in the Search feature:
 - ♦ Source Address of `<Model_Name>`
 - ♦ Base Event Count Score of `<Model_Name>`
 - ♦ Bytes Out of `<Model_Name>`
 - ♦ Bytes In of `<Model_Name>`

`<Model_Name>` corresponds to the model name being scored.

Defining and Building a Model

When you build the model, the feature aggregates events from the Events table by IP address, day of week, and hour of day for each five-minute time increment, and then calculates a sum for *EventCount*, *BytesIn*, and *BytesOut*. Outlier Analytics then creates conditional probability tables for sum of *EventCount*, sum of *BytesIn*, and sum of *BytesOut*.

- 1 Review the [considerations](#) for building a model.
- 2 Select **Configuration > Outlier**.
- 3 For **Create Model Configuration**, specify the criteria that you want to use for building the model.

For example:

- ♦ To define a specific subnet that represents a specific class of equipment (like server or data center), specify criteria similar to the following:

```
sourceAddress in subnet 10.1.1.0/24
```

- ♦ To model outbound HTTP/HTTPS traffic, specify criteria similar to the following:

```
destinationPort = 80,443
```

- 4 To name the model, type over **Model Name**.

The model name can contain letters, numbers, and underscores only. The name must start with an alpha character and cannot exceed 19 characters.

- 5 Specify a [time range](#) for the model.

Because of assumptions about the hours and days that comprise a model, do not specify a range that includes a shift in Daylight Savings Time.

Also, the timestamp for events always represents the [Normalized Event Time](#).

- 6 Select **Create**.

The created model appears in the **Available Models** table with a status of **Created**.

- 7 From the **Available Models** table, select the model that you want to build.

You can build only one model at a time.

- 8 Select **Build**.

- 9 To evaluate incoming events against the model, you must [start the scoring process](#).

Scoring a Model

You must have Administrative permissions to score a model.

Select **Insights > Outliers**.

After you [build](#) a model, you can start a **scoring process** that evaluates incoming events against the model. The process assigns a score that indicates the degree to which the incoming data varies from typical behavior. By default, Outlier Analytics selects the current date as the scoring start date.

You can only score one model at a time, but you can build another model while a different model is being scored.

To start the scoring process:

- 1 Select **Configuration** > **Outlier**.
- 2 From the **Available Models** table, select the model that you want to score.
The model must be in **Build Complete** status before you can score it.
- 3 Select **Score**.
- 4 Select the date for which you want to start the scoring process, then click **Start**.
Because of assumptions about the hours and days that comprise a model, do not use a model that you built with Daylight Savings Time data to score non-Daylight Savings Time data. Conversely, do not use a model that you built with non-Daylight Savings Time data to score Daylight Savings Time data.
- 5 (Conditional) To pause scoring because of performance or ingestion issues, select **Pause**.
If you selected a date in the past to start the scoring process, the scoring job runs frequently to catch up to the current date. To allow any running scoring jobs to complete, wait 15 minutes before performing any other action such as deleting a model or resetting scoring.
- 6 (Conditional) To resume the scoring process from the point at which you paused it, select **Resume**.
Alternatively, to restart the scoring process, select **Reset**.
- 7 To [view the scored data](#) when scoring completes, select **Insights** > **Outliers**.

Deleting a Model

You must have the Administrative permissions to delete a model.

When you delete a model, Outlier Analytics deletes the model definition and all scores that are based on that model.

- 1 Select **Configuration** > **Outlier**.
- 2 Select the model from the **Available Models** table that you want to delete.
- 3 Select **Delete**.

11 Viewing Anomalous Data in a Model

Select **Insights** > **Outliers**.

After you specify search criteria for the data that you want to view in the model, Outlier Analytics displays the top anomalous hosts that meet the criteria. When you select a host from the **Top Anomalous Hosts** table, the feature generates charts that provide more information about the anomaly scores. The scores are calculated for five-minute chunks, so each source address can have multiple outlier scores each hour. When listing the top anomalous hosts, Outlier Analytics shows the maximum scores for each source address for each hour. If the specified search criteria included a filter, the scores represent results after being filtered.

- ♦ [“Understand the Provided Analytics Charts” on page 99](#)
- ♦ [“Further Investigate Anomalies” on page 100](#)
- ♦ [“View a Scored Model” on page 100](#)

Understand the Provided Analytics Charts

Each Outlier Analytics model includes the following charts:

Outlier Scores History

Compares anomaly scores of the top anomalous hosts for one week from the specified **End time**.

Use this chart if you suspect a lateral attack. To view details about the score for a specific date and hour, hover over the corresponding area in the chart.

Selected Anomalous IP

Shows the anomaly score for the host that you selected for two weeks from the specified **End time**.

If you suspect that a host is under attack (for example, from ex-filtration malware), use this chart to study the behavior of the IP address over time and identify anomalous patterns. To view details about a data point, hover over it.

Selected Anomaly Hour

Compares the anomaly score for the host that you selected to the top 30 hosts for the anomaly hour.

If you suspect that a network is under attack (for example, a denial of service attack), use this chart to study the behavior of other top 30 hosts during the anomaly hour. To view more details, hover over a bar in the chart, click and drag to move within the chart, and double-click to reset it to its default view.

Further Investigate Anomalies

After you view the outlier data, you can use the action available from the grid rows in the **Top Anomalous Hosts** table to further investigate anomalies:

Search for <IP_Address>

Searches events for the host and time range for which you selected to view scoring data and displays the results on the **Search** page.

View a Scored Model

- 1 Select **Insights > Outliers**.
- 2 Specify the outlier metric that you want to view: **EventCount**, **BytesIn**, or **BytesOut**.
- 3 For the search query, specify any of the following criteria that you want to apply to the data:
 - ♦ Base Event Count Score of
 - ♦ Bytes In Score of <Model_Name>
 - ♦ Bytes Out Score of <Model_Name>
 - ♦ Source Address of <Model_Name>
 - ♦ Start Time of <Model_Name>

- 4 Select **Detect**.

- 5 Specify a valid **time range** for which to view the scored data.

Time range selector displays the valid date range in the date selection area to ensure that you specify a valid date range. Scoring data is performed hourly so the time range for detection is in an hourly format (YYYY-MM-DD HH). End time hour is inclusive. If the end time is 2019-05-21 05, the scoring data from 2019-05-21 05:00-06:00 will be included. To help you select time range for detection, the time range selector displays **Score Available Range**.

- 6 Wait while Outlier Analytics processes the request and generates the **Top Anomalous Hosts** table and the **Outlier Scores History**.

CAUTION: If Outlier Analytics retrieves a large amount of data, the search might pause. You must allow the feature to populate the **Top Anomalous Hosts** table before you select the **Play** button to resume the search. Otherwise, the table will not be displayed.

- 7 (Optional) To generate the remaining charts, select a row in the **Top Anomalous Hosts** table.
- 8 (Optional) To use the filter action in your investigation, complete the following steps:
 - 8a Right-click a row in the grid.
 - 8b Select **Search for <IP_Address>**.

IV

Managing the Quality of Your Data

Select [Insights](#) > [Data Quality](#).

Data Quality Dashboard provides detailed information about the gap between [Device Receipt Time](#) from the raw event itself versus the [Normalized Event Time](#).

Data Quality Dashboard identifies the sources that cause issues with the data. Based on the information analyzed through the Data Quality Dashboard, you can accurately mitigate the problem. This feature also provides history of your data over time.

- ♦ [Chapter 12, “Understanding the Data Quality Insights,” on page 103](#)
- ♦ [Chapter 13, “Understanding How Data Quality is Calculated,” on page 105](#)
- ♦ [Chapter 14, “Analyzing Data Quality,” on page 107](#)

12 Understanding the Data Quality Insights

Content in the [Data Quality Dashboard](#) is divided into categories that represent how big the gaps are between [Device Receipt Time](#) and [Normalized Event Time](#):

Future Events

Indicates that events have a future timestamp in them. This category uses the following formula:

Normalized Event Time (NET) - Device Receipt Time (DRT) < 0

Past Events

Indicates that events have a past timestamp in them. This category uses the following formula:

Normalized Event Time (NET) - Device Receipt Time (DRT) > 0

Active Events

Indicates that your events have a timestamp within the database's active time-frame. This category uses the following formula:

Normalized Event Time (NET) - Device Receipt Time (DRT) = 0

13 Understanding How Data Quality is Calculated

Data Quality is calculated and aggregated every one hour, including all events that arrive in the database within the same hour. For example, the aggregated information at 10:00 AM includes all data from 10:00:00.000 to 10:59:59.999, inclusively. The time of the aggregation process depends on when the product was installed or upgraded:

- ♦ During a fresh installation, the process creates a new table to store Data Quality overtime with data sources information. The feature schedules the aggregation process at the tenth minute of every hour. For example, if a fresh install was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM and every one hour after that.
- ♦ After an upgrade, previous data will be dropped because they are no longer relevant to new categories. For example, if an upgrade was performed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM to aggregate all events from 9:00:00.000 to 9:59:59.999 AM, inclusive. Then it will run every one hour after that.

If you switch to a different database, you would need to wait for a few minutes before accessing the Data Quality page again.

14 Analyzing Data Quality

Select [Insights](#) > [Data Quality](#).

The Dashboard provides the following visualizations to help you gain insight into quality of your data.

Date Picker Filter

Provides options to filter the [time range](#) for the entire Data Quality Dashboard page, including built-in Quick Ranges and a Custom Range. By default, the Dashboard displays data per the [Last 7 days](#) setting.

If the [Cron Job](#) has not been run yet, the charts would display no data.

Data Timeseries

Represents, in a stacked area chart, how data is distributed among the [Categories](#) by percentage over time.

Source Agents

This visualization group consists of the following components:

Category Selector

Displays data sources in each of the three [Data Categories](#).

Top 10 Agents

Represents the percentages of up to 10 top agents with the greatest amount of events under the selected Data Categories. To see the IP address, hostname, and number of events of each source, hover over each donut piece. If you click a donut piece, Outlier Analytics displays additional details in the Data Timeseries side chart.

Hourly Event Volume

Shows, in a bar chart, the number of events from a data source that contributed to the selected Data Categories. If available, the source with the highest number of events will be displayed by default.



Ensuring Data Compliance

Recon provides Compliance Packs to help you comply with a broad set of legal and governmental regulations that require your enterprise to organize and manage sensitive data and institute a strong IT governance program. Designed around best practices, these packages provide a comprehensive method for assessing and monitoring internal controls, such as access control changes, administrative activity, log-in monitoring, and change and risk management. The packages automatically map these technical checks to the relevant standard using policy and risk-relevant operational context so you can focus on key services and business processes and address critical audit points.

- ♦ [Chapter 15, “Ensuring Compliance with GDPR Standards,” on page 111](#)
- ♦ [Chapter 16, “Ensuring Compliance with ISO-27002,” on page 127](#)
- ♦ [Chapter 17, “Ensuring Compliance with PCI DSS,” on page 131](#)

You must purchase, then import each Compliance Pack to the [Reports repository](#). For more information about the packs, see the [Recon documentation site](#).

15 Ensuring Compliance with GDPR Standards

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [GDPR](#).

The European Union (EU) adopted the General Data Product Regulation (GDPR) to ensure that businesses and organizations protect individuals' data privacy and security. If your enterprise processes the personal data of EU citizens or residents or offers goods and services to such individuals, then you must comply with the GDPR. The regulation sets out standards for any action, automatic or manual, that processes a person's data. These standards include requiring that data controllers and data processors – the individuals in your enterprise or third-party organizations who control, manage, or make decisions about data processing – must be able to demonstrate that they are GDPR compliant.

To help you comply or prove compliance with GDPR, Recon provides the **Compliance Pack for GDPR**. For more information about adding the pack to the [Reports repository](#), see the [Solutions Guide for ArcSight Recon Compliance Pack for GDPR](#). The guide includes information about identifying assets that must comply with GDPR.

This package includes the following dashboards and reports, organized by GDPR objectives:

Category	Dashboards	Reports
Access Activity	After Hours Access Activity on GDPR Systems Overview Authorization Changes on GDPR Systems Overview Failed Access Activity by GDPR Asset Failed Access Activity on GDPR Systems by User Failed Access Activity on GDPR Systems Overview Failed Access Relationship on GDPR Systems Overview	After Hours Access Activity on GDPR Systems Summary Authorization Changes Summary on GDPR Systems Failed Access Activity by GDPR Assets Failed Access Activity on GDPR Systems by Users Failed Access Activity on GDPR Systems Summary
Access Activity - Potential Regulatory Exposure	n/a	Potential Regulatory Exposure on GDPR Systems
Access Activity - Threat User Analysis	n/a	Admin Activity from Compromised GDPR Systems Anti-Virus Disabled on GDPR Systems Summary Audit Log Cleared on GDPR Systems Summary Threats Executed against GDPR Systems Summary

Category	Dashboards	Reports
Admin Activity	n/a	Users Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment
Attack Surface Analysis - Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL and TLS Vulnerabilities on GDPR Systems Vulnerabilities on GDPR Systems Overview Vulnerable GDPR Assets by Vulnerability Type XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Attack Surface Analysis - Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems
Corporate Governance	Access Activity on GDPR Systems Overview Geo Access Activity on GDPR Systems Overview Physical Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary After Work Hours Physical Access Activity on GDPR Systems Summary Physical Access Activity on GDPR Systems Summary

Category	Dashboards	Reports
Regulatory Exposure	Data Flow to GDPR Systems Data Flow from GDPR Systems Data Flow from GDPR Systems to non EU Data Flow from non EU to GDPR Systems GDPR Systems Communication Overview GDPR Systems Communication with non EU Countries High Risk Events on GDPR Systems Overview Policy Violations on GDPR Systems Overview Threat Relationship on GDPR Systems Overview Threats on GDPR Systems Overview	Data Flow from GDPR Systems Summary Data Flow from GDPR to non EU Summary Data Flow from non EU to GDPR Systems Summary Data Flow to GDPR Systems Summary High Risk Events on GDPR Systems Summary Policy Violations on GDPR Systems Summary Threats on GDPR Systems Summary
Threat Analysis - Data Store Risk	n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems

Category	Dashboards	Reports
Threat Analysis - Internet Threat Analysis	Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Access Activity

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity**.

As a data controller or data processor, you need to track access to **GDPR systems**, which collect, store, transfer, use, and organize data related to EU citizens or residents.

- ♦ [“Access Activity” on page 114](#)
- ♦ [“Regulatory Exposure” on page 116](#)
- ♦ [“Threat User Analysis” on page 116](#)

Access Activity

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Access Activity** > **Access Activity**.

To comply with GDPR, you might want to track accounts that have been accessing systems that store or process users’ personal data. A high number of failed access attempts can indicate malicious activity. Also, to prevent a malicious user from accessing sensitive data, you should know when and what type of authorization changes occur on those systems.

After Hours Access Activity on GDPR Systems Summary

Reports the number of times and the accounts that accessed GDPR systems outside of regular hours, such as accessing a server on the weekend. The table provides results by the account and its associated server, and the target server accessed. This report relates to GDPR Articles 5 and 25 and Recital 49.

By default, the report uses the following time ranges to check for “after hours” access:

- ♦ 12 a.m. to 7 a.m. Monday through Friday
- ♦ 18 p.m. (6 p.m.) to 12 a.m. Monday through Friday
- ♦ All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Authorization Changes Summary on GDPR Systems

Reports the number and type of authorization change events that occur on GDPR systems over time. The table provides results by the number of times each account made a change, the type of change, the affected GDPR system, and the outcome of the change such as 'success.' This report relates to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Failed Access Activity by GDPR Assets

Reports the number of times access to a GDPR asset failed. The chart shows the top GDPR assets with failed access attempts. For each GDPR asset, the table provides results by the number of failed events, user accounts with failed attempts, and the number of IP addresses associated with the failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems by Users

Reports the number of times users failed to access a GDPR system. The chart shows the users with the most failed access attempts. The table provides results by number of failed events, GDPR assets affected, and IP addresses associated with the failed events for each user with a failed attempt. This report relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Activity on GDPR Systems Summary

Reports the number attempts that failed to access a GDPR system over time. For each failed attempt, the table provides results by user account, the account's IP address and country, the target server's IP and host name, and the number of failed events. This report relates to GDPR Articles 5 and 25 and Recital 49.

After Hours Access Activity on GDPR Systems Overview

Provides, in charts and a table, an overview of accounts that access GDPR systems outside of regular hours, such as accessing a server on the weekend. You can view the targeted systems, users, and source IPs that generate the most events. This dashboard relates to GDPR Articles 25, 30, and 32 and Recital 82.

By default, the dashboard uses the following time ranges to check for "after hours" access:

- ♦ 12 a.m. to 7 a.m., Monday through Friday
- ♦ 18 p.m. to 12 a.m., Monday through Friday
- ♦ All day on Saturday and Sunday

Authorization Changes on GDPR Systems Overview

Provides an overview of events that indicate authorization change attempts on GDPR Systems. Relevant to GDPR Articles 5, 18, 24, 29, and 32 and Recital 39.

Failed Access Activity by GDPR Asset

Provides, in charts and a table, an overview of failed access activity on the specified GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one IP address, Mac address, or host name in lowercase.

Failed Access Activity on GDPR Systems by User

Provides, in charts and a table, an overview of failed access activity by user. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

You must specify at least one user account in lowercase.

Failed Access Activity on GDPR Systems Overview

Provides an overview of failed access activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Failed Access Relationship on GDPR Systems Overview

Provides an overview of the relationship between source and destination addresses and users on events that indicate a failure login activity on GDPR systems. This dashboard relates to GDPR Articles 5 and 25 and Recital 49.

Regulatory Exposure

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Access Activity** > **Regulatory Exposure**.

As part of your compliance measures, you most likely track access events that might have compromised user data, thus breaching GDPR regulations.

Potential Regulatory Exposure on GDPR Systems

Reports the GDPR systems that might have been exposed to a regulatory infraction due to user access activities. The chart shows the systems with the most events. The table provides results by the event name and time by GDPR system. This report relates to GDPR Article 32 and Recital 49.

Threat User Analysis

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Access Activity** > **Threat User Analysis**.

User activities such as changing authorizations or clearing audit logs often indicate malicious activities or potential vulnerabilities. Run the following reports to check for threat activities on your GDPR systems.

Admin Activity from Compromised GDPR System

Reports events associated with administrative activities that occur on GDPR systems. For example, users are executing commands or changing authorizations. The chart shows activity over time. The table provides results by time, user, affected GDPR asset, activity type, and the number of events. This report relates to GDPR Articles 30 and 32 and Recital 49.

Anti-Virus Disabled on GDPR Systems Summary

Reports how often anti-virus services have been stopped or paused on GDPR systems over time. A malicious user might pause an anti-virus service before running an illegal command or script or downloading or installing malicious programs. The table provides results by time, GDPR system, affected service, and number of events. This report relates to GDPR Article 32 and Recital 49.

Audit Log Cleared on GDPR Systems Summary

Reports the audit log has been cleared on GDPR systems. The chart shows the number of events over time. The table provides results by date, user, and host. This report relates to GDPR Articles 5 and 25 and Recital 49.

Threats Executed against GDPR Systems Summary

Reports how often GDPR systems have been threatened. The chart shows the number of events over time. The table provides results by date, system IP address, threat technique, event name, and number of events. This report relates to GDPR Article 32 and Recital 49.

Admin Activity

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Admin Activity** > **Provisioning Activity**.

Administrators can create and remove users. These admins might inadvertently or deliberately add users to a system or group, giving users access to sensitive systems and information. Alternatively, a malicious user with access to an admin account might attempt to create users for later access or remove necessary accounts. To comply with GDPR, you should track administrator activities related to user creations, deletions, and group assignments.

User Creations on GDPR Environment

Reports the number of user accounts created over time and by whom in the GDPR environment. The table provides results by date, created account, user creating the account, and their domains. This report relates to GDPR Articles 5, 6, and 7 and Recitals 78, 82, and 84.

User Deletions on GDPR Environment

Reports the number of user accounts deleted over time and by whom in the GDPR environment. The table provides results by date, the deleted account, user deleting the account, and their domains. This report relates to GDPR Article 17 and Recital 66.

Users Added to a Group on GDPR Environment

Reports the number of user accounts added to groups over time and by whom in the GDPR environment. The table provides results by date, subject, user adding the account, and affected group. This report relates to GDPR Articles 5, 6, 7, and 32 and Recitals 78, 82, and 84.

You must specify the name of a user group in lowercase.

Users Removed from a Group on GDPR Environment

Reports the number of user accounts removed group groups over time and by whom in the GDPR environment. The table provides results by date, subject, user removing the account, and affected group. This report relates to GDPR Articles 17 and 32 and Recital 66.

You must specify the name of a user group in lowercase.

Attack Surface Analysis

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Attack Surface Analysis**.

Each point entry in your environment, which unauthorized users or programs can exploit, increases the environment's attack surface. This package helps you analyze the extent of the environment's vulnerability.

- ♦ [“Attack Surface Identification” on page 118](#)
- ♦ [“Security Controls Risk Identification” on page 120](#)

Attack Surface Identification

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Attack Surface Analysis** > **Attack Surface Identification**.

To prevent data breaches, you need to know how much of your GDPR environment is vulnerable to attack. Use the following dashboards and reports to identify, and thus reduce, your environment's attack surface.

High Risk Vulnerabilities on GDPR Systems

Reports the high-risk vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems

Reports the information leakage vulnerabilities detected in the GDPR environment. The chart shows the systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems

Reports the password and authentication weaknesses detected in the GDPR environment. The chart shows the number of events over time. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems

Reports the SQL injection vulnerabilities detected in the GDPR Environment. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL or TLS Vulnerabilities on GDPR Systems

Reports the SSL and TLS vulnerabilities detected in the GDPR Environment. Malicious users can exploit vulnerabilities in SSL and TLS. For example, the [Heartbleed Bug](#) is a known SSL vulnerability. The chart shows the systems with the most detected vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Unpatched GDPR Systems

Reports the GDPR Systems with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The chart shows the systems with the most missing security patches. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerability Summary by CVE ID

Reports the vulnerabilities detected in the GDPR environment by specific CVE ID. The chart shows the number of assets with the specified vulnerability over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify a CVE ID.

Vulnerability Summary by GDPR Asset

Reports the vulnerabilities detected on a specific GDPR asset. The chart shows the number of vulnerabilities detected over time. The table provides results by host name, IP address, Mac address, signature ID, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

You must specify one GDPR asset by host name, IP address, or Mac address.

Vulnerability Summary on GDPR Systems

Reports the vulnerabilities detected in the GDPR environment. The chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems

Reports the cross-site scripting (XSS) vulnerabilities detected in the GDPR environment. Vulnerabilities associated with XSS enable malicious users to inject code in legitimate web pages or applications that executes harmful scripts in the user's web browser when the browser parses data. The chart shows the assets with the most detected vulnerabilities. The table provides results by asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

High Risk Vulnerabilities on GDPR Systems

Provides an overview of high-risk vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Information Leakage Vulnerabilities on GDPR Systems

Provides an overview of information leakage vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Password and Authentication Weaknesses on GDPR Systems

Provides an overview of password and authentication Weaknesses reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SQL Injection Vulnerabilities on GDPR Systems

Provides an overview of SQL Injection vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

SSL and TLS Vulnerabilities on GDPR Systems

Provides an overview of SSL and TLS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerabilities on GDPR Systems Overview

Provides an overview of vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Vulnerable GDPR Assets by Vulnerability Type

Provides an overview of vulnerabilities reported on GDPR systems by Type. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

XSS Vulnerabilities on GDPR Systems

Provides an overview of XSS vulnerabilities reported on GDPR systems. This dashboard relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Security Controls Risk Identification

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [GDPR](#) > [Reports](#) or [Dashboards](#) > [GDPR Attack Surface Analysis](#) > [Security Controls Risk Identification](#).

Not all malicious users want to breach your systems to access or manipulate data. Some might want to disrupt service and deny users access to information. However, a [denial-of-service \(DoS\)](#) attack might indicate a future threat to your environment.

DoS Attacks Against GDPR Systems

Reports potential DoS events against databases in the GDPR environment. The chart shows the number of attacks over time. The table provides results by the source IP and port, the target IP and port, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

DoS Attacks Against GDPR Systems

Provides a summary overview of DoS Attacks against GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

Corporate Governance

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [GDPR](#) > [Reports](#) or [Dashboards](#) > [GDPR Corporate Governance](#) > [Record Keeping](#).

In some environments, sensitive data is stored in file cabinets or archives. To ensure compliance with GDPR, your organization might control access to the physical environment where these records are kept. Use the following dashboards and reports to track access to these environments.

Access Activity on GDPR Systems Summary

Reports access events to GDPR systems. The chart shows access by country over time. The table provides results by user, source IP and country, target IP and host, and number of events. This report relates to GDPR Articles 30, 32, and 25, and Recital 82.

After Work Hours Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as buildings, during after work hours. The chart shows both failed and successful access by user and building. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

By default, the report uses the following time ranges to check for “after hours” access:

- ♦ 12 a.m. to 7 a.m., Monday through Friday
- ♦ 18 p.m. (6 p.m.) to 12 a.m., Monday through Friday
- ♦ All day on Saturday and Sunday

However, you can modify the time ranges by editing the filters for the report. The time range uses 24-hour values.

Physical Access Activity on GDPR Systems Summary

Reports access to physical GDPR systems, such as building. The chart shows both failed and successful access by building over time. The table provides results by date, user, building, result, and number of attempts. This report relates to GDPR Articles 24 and 32 and Recital 49.

Access Activity on GDPR Systems Overview

Provides an overview of access events reported on GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Geo Access Activity on GDPR Systems Overview

Provides an overview of GEO access activity to GDPR systems. This dashboard relates to GDPR Articles 30, 32, and 25 and Recital 82.

Physical Access Activity on GDPR Systems Overview

Provides an overview of physical access events reported on GDPR systems, by default “after Work Hours” charts defined from 12 a.m. to 7 a.m. and 18 p.m. to 12 a.m. every Monday to Friday and the whole days of Saturday and Sunday, those can be re-configured to different values using this dashboard charts components filter. This dashboard relates to GDPR Articles 24 and 32 and Recital 49.

Regulatory Exposure

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > **Reports** or **Dashboards** > **GDPR Regulatory Exposure** > **Composite Regulatory Exposure**.

To comply with GDPR, you might need to track how data flows among GDPR system, and from systems in non-EU countries.

Data Flow from GDPR Systems Summary

Reports events that detect the flow of data from GDPR systems. The chart shows the GDPR systems with the most data flowing outward. The table provides results by the IP address of the GDPR source system, the target IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU Summary

Reports events that detect the flow of data from GDPR systems to systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing outward by country. The table provides results by the IP address of the GDPR source system, the IP address of the non-EU system, the country code of the target system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems from systems in non-European Union countries. The chart shows the GDPR systems with the most data flowing in by country of origin. The table provides results by the IP address and country code of the source system, the IP address of the GDPR system, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

Data Flow to GDPR Systems Summary

Reports events that detect the flow of data to GDPR systems. The chart shows the GDPR systems with the most data flowing into them. The table provides results by the IP address of the source system, the target (GDPR system) IP address and host, and the number of events detected. This report relates to GDPR Articles 30, 32, 45, 46, and 49 and Recital 82.

High Risk Events on GDPR Systems Summary

Reports high-risk events that involve GDPR systems. The chart shows the targeted GDPR systems with the most high-risk events. The table provides results by the source IP and host of the events, the targeted IP and host GDPR system, the user, and number of events detected. This report relates to GDPR Articles 32 and 83 and Recital 49.

Policy Violations on GDPR Systems Summary

Reports the number of policy violation events on GDPR systems over time. The table provides results by source IP address, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and 83 and Recital 49.

Threats on GDPR Systems Summary

Reports the number of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems over time. The table provides results by IP and Mac address of the source system, the IP address and host of the target GDPR system, user, and number of events. This report relates to GDPR Articles 32 and Recital 49.

Data Flow to GDPR Systems

Provides a summary overview of data flow to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems

Provides a summary overview of data flow from GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from GDPR Systems to non EU

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

Data Flow from non EU to GDPR Systems

Provides a summary overview of data flow from non EU to GDPR Systems. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication Overview

Provides an overview of GDPR Systems communications. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

GDPR Systems Communication with non EU Countries

Provides an overview of GDPR Systems communications with non EU Countries. This dashboard relates to GDPR Articles 30, 46, 32, 45, 46, and 49 and Recital 82.

High Risk Events on GDPR Systems Overview

Provides an overview of high risk events related to GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Policy Violations on GDPR Systems Overview

Provides an overview of policy violation events related to GDPR systems. This dashboard relates to GDPR Articles 32 and 83 and Recital 49.

Threat Relationship on GDPR Systems Overview

Provides an overview of relationship between source and destination addresses on events which indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threats on GDPR Systems Overview

Provides an overview of events that indicate compromise, reconnaissance, hostile, or suspicious activity on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

Threat Analysis

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis**.

GDPR requires that your enterprise establish technical and organizational standards that ensure appropriate security-to-risk levels. To create appropriate security measures, you need to assess the risks and the severity of threats to sensitive data.

- ♦ [“Data Store Risk” on page 123](#)
- ♦ [“Internet Threat Analysis” on page 125](#)

Data Store Risk

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Threat Analysis** > **Data Store Risk**.

As part of your threat analysis, you should assess the vulnerability of data storage systems.

Attacks Against Databases on GDPR Systems

Reports events that indicate compromise, reconnaissance, hostile, or suspicious activity against GDPR systems databases over time. The table provides results by the source GDPR IP address, IP address and host of the target system, name of the event, and number of events. This report relates to GDPR Article 32 and Recital 49.

Cassandra Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Apache Cassandra on GDPR systems. Apache Cassandra is a free and open-source, distributed, wide-column store, NoSQL database management system. The chart shows the GDPRs reporting the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

CRM and ERP Vulnerabilities on GDPR Systems

Reports vulnerabilities detected on GDPR systems related to CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) software. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Database Configuration Changes on GDPR Systems

Reports changes to the database configuration in the GDPR environment. The chart shows the GDPR systems with the most changes. The table provides results by host system, database change, the type of change, agent severity, and date of the most recent event. This report relates to GDPR Article 32.

Database Weaknesses on GDPR Systems

Reports vulnerabilities in databases detected in the GDPR environment over time and by severity. The table provides results by GDPR asset, signature ID, description of the vulnerability, agent severity, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Elasticsearch Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Elasticsearch on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

IBM Db2 Vulnerabilities on GDPR Systems

Reports vulnerabilities related to IBM Db2 on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MariaDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MariaDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Microsoft SQL Server Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Microsoft SQL Server on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MongoDB Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MongoDB on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

MySQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to MySQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Oracle Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Oracle on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

PostgreSQL Vulnerabilities on GDPR Systems

Reports vulnerabilities related to PostgreSQL on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Redis Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Redis on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset, signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Internet Threat Analysis

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [GDPR](#) > [Reports](#) or [Dashboards](#) > [GDPR Threat Analysis](#) > [Internet Threat Analysis](#).

As part of your threat analysis, you should assess the vulnerability of firewalls, places where information might leak, and existence of malware on your GDPR systems.

Firewall Blocked Events in GDPR Environment

Reports firewall blocked events in the GDPR environment. The chart shows the number of events by time and target port. If you pro-actively monitor the firewalls in your enterprise, you can identify problems at an early stage and prevent network attacks. The table provides results by source IP address and port, the targeted GDPR IP address and port, and the number of events. This report relates to GDPR Article 32 and Recital 49.

Information Leaks from GDPR Systems

Reports events that indicate information leaks on GDPR systems over time. The table provides results by date, event name, source IP address and port, the targeted GDPR IP address and port, and the user. This report relates to GDPR Articles 32, 33, and 34 and Recitals 49, 85, and 86.

Malware Found on GDPR Systems

Reports malware found on GDPR systems. The chart shows the systems with the most malware activity. The table provides results by GDPR asset, malware program, name of the event, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Malware on GDPR Systems

Provides an overview of Malware reported events on GDPR Systems. This dashboard relates to GDPR Articles 32, 33, and 34 and Recitals 49 and 83.

MITRE ATT&CK on GDPR Systems by GDPR Asset

Provides an overview of MITRE ATT&CK events by GDPR asset. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems by MITRE ID

Provides an overview of MITRE ATT&CK events reported on GDPR Systems by MITRE IDs. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK on GDPR Systems Overview

Provides an overview of MITRE ATT&CK events reported on GDPR Systems. This dashboard relates to GDPR Article 32 and Recital 49.

MITRE ATT&CK Relationship on GDPR Systems Overview

Provides an overview of the relationship between different event entities on MITRE ATT&CK events reported on GDPR systems. This dashboard relates to GDPR Article 32 and Recital 49.

16 Ensuring Compliance with ISO-27002

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [IT GOV](#) > [ISO-27002](#).

To comply with ISO 27002 guidelines, your enterprise needs to establish and follow information security standards and policies. The guidelines help you identify and implement the controls needed to secure data. You can check the security controls in your enterprise against one or more specific ISO 27002 control set, such as *Information Security Policies* or *Asset Management*.

To help you comply with the *Operations Security* control set, Recon provides the **Compliance Pack for IT Governance**. For more information about adding the pack to the [Reports repository](#), see the [Solutions Guide for ArcSight Recon Compliance Pack for IT Governance](#).

This package includes the following reports for the *Operations Security* control set:

- ♦ [Administrative Actions All Events](#)
- ♦ [Administrative Logins and Logouts](#)
- ♦ [Application Configuration Modification](#)
- ♦ [Audit Log Cleared](#)
- ♦ [Changes to Operating System](#)
- ♦ [Device Configuration Changes](#)
- ♦ [Device Logging Review](#)
- ♦ [Exploit of Vulnerabilities](#)
- ♦ [Failed Administrative User Logins](#)
- ♦ [Failed User Logins](#)
- ♦ [Logins to Database Machines](#)
- ♦ [Machines Conducting Policy Breaches](#)
- ♦ [Successful Administrative User Logins](#)
- ♦ [Successful User Logins](#)
- ♦ [User Actions Summary](#)
- ♦ [User Logins and Logouts](#)
- ♦ [Virus Infected Machines](#)

12 – Operations Security

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [IT GOV](#) > [ISO-27002](#) > [Reports](#) > [ISO 12 - Operations Security](#).

Section 12: Operations security of the ISO 27002 standard focuses on ensuring that the facilities that store and process information are protected from malware, data loss, and the exploitation of technical vulnerabilities. Use the following reports to check for compliance with the standard.

Administrative Actions All Events

Reports the accounts that have performed the most administrative actions. The table provides results by admin account, destination IP address, the name and ID of the detected event, the affected product, the number of events, and date of the most recent event.

Administrative Logins and Logouts

Reports the hosts that have had the highest number of logins and logouts by administrative accounts. The table provides results by the name of the event, the admin account, the IP address and name of the affected host, the action taken, the number of events, and the date of the most recent event.

Application Configuration Modification

Reports the applications that have had the highest number of configuration changes. For example, a user might have updated a license file or a program setting. The table provides results by the vendor and product modified, the IP address and zone of the host system, and the date that the modification occurred.

Audit Log Cleared

Reports the number of audit logs that have been cleared over time. The table provides results by the date, IP address and host of the affected system, the affected account, the source account that cleared the audit log, and the affected device.

Changes to Operating System

Reports the 10 hosts with the most changes to the operating system. Detected modifications might be to the security options or OS accounts. The table provides results by IP address and name of the affected host system, the device product and vendor that was changed, and the destination zone.

Device Configuration Changes

Reports the type and number of modifications made to devices in the network. The table provides results by the date, time, event name, affected product, and the host where the changes occurred.

Device Logging Review

Reports the devices with the most logging events, such as a database. The table provides results by the device host name and address, the vendor and product affected, number of events detected for that product, and the date of the most recent event.

Because this report queries the logging activity from all devices, it will have a performance impact each time that you run it.

Exploit of Vulnerabilities

Reports the number of detected events where a user might have exploited a well-known vulnerability. For example, an IDS might report an event associated with a Unicode vulnerability. The table provides results by the vulnerability, the affected host, and the number of detected events.

Failed Administrative User Logins

Reports the number of failed logins by administrative accounts over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and the date of the most recent event.

Failed User Logins

Reports the number of failed logins over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and the date of the most recent event.

Logins to Databases Machines

Reports the user accounts with the most attempts to log in to databases in your environment. The table provides results by the user account, the affected host, the number of attempts, whether the attempt was successful, and date of the most recent event.

Machines Conducting Policy Breaches

Reports the systems with the most policy breaches, which match the category technique of / *Policy/Breach*. The table provides results by the device group, affected vendor and product, the IP address and name of the host, and date of the breach.

Malicious Code Sources

Reports the devices that where malicious code source has been detected. The table provides results by the event name, the affected device, the source device, affected product, the category of the malicious code, and the outcome.

Successful Administrative User Logins

Reports the number of successful logins by administrative accounts over time. The table provides results by account name, the name and IP address of the host where the logins occurred, the affected product or operating system, the number of successful logins, and the date of the most recent event.

Successful User Logins

Reports the number of successful logins over time. The table provides results by account name, the name and IP address of the host where the logins occurred, the affected product or operating system, the number of successful logins, and the date of the most recent event.

User Actions Summary

Reports the non-administrative accounts with the most actions taken. For example, a user might delete an infected file. The report provides results by the source account, the affected account, the name of the event, the IP address where the action occurred, the affected product, the outcome of the user's action, the number of times that the action was detected, and the date of the most recent event.

Run this report with caution, as it can generate enormous amounts of data. This report will not include events in which both source and destination users are null.

User Logins and Logouts

Reports the user accounts that log in and out the most. The table provides results by the name of the login action and category, the user account, the IP address, name, and zone of the affected system, and the date of the event.

Virus Infected Machines

Reports the systems with the most detected viruses by affected product. The table provides results by the virus name, the affected system and product, and the date of the event.

17 Ensuring Compliance with PCI DSS

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [PCI](#).

The [PCI Security Standards Council](#) has established standards to ensure the security of payment account data. To help you comply with Requirements 1, 2, 4, and 10 of the PCI Data Security Standards, Recon provides the **Compliance Pack for PCI**. For more information about adding the pack to the [Reports repository](#), see the [Solutions Guide for ArcSight Recon Compliance Pack for PCI](#).

This pack includes the reports organized by the following PCI requirements:

Category	Reports
Firewall Configuration	Accessed Ports Through Firewall Blocked Inbound Traffic to Card Holder Data Environment Blocked Outbound Traffic from Card Holder Data Environment External to Internal PCI Systems Firewall Configuration Changes Inbound Traffic to the Card Holder Data Environment Outbound Traffic from the Card Holder Data Environment Unauthorized Inbound Traffic to DMZ Unauthorized Outbound Traffic From Card Holder Data Environment
Default Security Parameters	Default Vendor Accounts Internal PCI Systems to External Misconfigured Systems Network Routing Configuration Changes Personal Firewall Installed Private IP Addresses Disclosure Software Inventory Unauthorized Inbound Traffic to Card Holder Data Environment Unencrypted Administrative Accesses VPN Configuration Changes
Encryption Transmission	Cryptographic Hash Algorithm Related Vulnerabilities Cryptographic Public Key Related Vulnerability Detected SSL or TLS Vulnerabilities TLS BREACH Vulnerabilities TLS CRIME Vulnerabilities Wireless Encryption Violations

Category	Reports
Track and Monitor Data Access	Account Creation Account Deletion Account Modification User Group Creation User Group Deletion

Firewall Configuration – Requirement 1

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > **PCI Reports** > **Requirement 1:Firewall Configuration**.

PCI Requirement 1 requires that you install and maintain a firewall configuration to protect card holder data. **Firewalls** control computer traffic in and out of your network, as well as to and from sensitive areas within secure or sensitive internal networks. To prove compliance with PCI DSS, you must monitor the firewalls at Internet connections and between any demilitarized zones (DMZs). You must also monitor the devices that manage traffic.

Accessed Ports Through Firewall

Reports the firewalls that allowed the most traffic by port number. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; number of events; and the firewall rule number that triggered the event.

Blocked Inbound Traffic to Card Holder Data Environment

Reports the destination ports with inbound traffic that has been blocked the most often. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; the protocol used, number of events; and date of the most recent event.

Blocked Outbound Traffic from Card Holder Data Environment

Reports an overview of blocked outbound traffic over time. The table provides results by blocked outbound traffic per firewall. It lists the IP addresses for the firewall, the source system, and the destination system; the source and destination zones; affected port; and date of the most recent event.

External to Internal PCI Systems

Reports the external systems that are communicating directly with PCI internal systems most often. The table provides results by the IP addresses and zones of the source and destination systems, the affected port, protocol used, and the number of events. PCI standards expects that your enterprise can justify this type of traffic.

Firewall Configuration Changes

Reports the firewalls and devices where the configuration has changed. The table provides results by the IP address, product, and vendor of the device that was changed; the name and rule related to the change; the number of changes detected; and the date of the most recent event.

Inbound Traffic to the Card Holder Data Environment

Reports the five systems that allowed the most inbound traffic by destination address and port. The table provides results by the IP addresses for the firewall, the source system, and the destination system; the affected port; the protocol used; number of events; and date of the most recent event.

Outbound Traffic from the Card Holder Data Environment

Reports the systems that allowed outbound traffic by destination IP address. The table provides results by the IP addresses for the device, the source system, and the destination system; the affected port; the protocol used; number of events; and date of the most recent event.

Unauthorized Inbound Traffic to DMZ

Reports the systems with the highest amount of unauthorized inbound traffic. The table provides results by the IP addresses for the device, the source system, and the destination system; the source zone; affected port; number of events; and date of the most recent event.

Unauthorized Outbound Traffic From Card Holder Data Environment

Reports the ports with the most unauthorized traffic. The table provides results by the IP addresses for the device, the source system, and the destination system; the destination zone; the affected port; the protocol used; and number of events.

Default Security Parameters – Requirement 2

Select **Reports > Portal > Repository > Standard Content > PCI > PCI Reports > Requirement 2:Default Security Parameters**.

PCI Requirement 2 addresses the use of vendor-supplied default settings, such as passwords and account names. These are known values and can be exploited by malicious users. While devices and firewalls installed by IT administrators might have strong security process, users who install software and add devices might not follow good security practices.

Use the following reports to check for default security parameters in your environment.

Default Vendor Accounts

Reports default vendor accounts by username. The table provides results by the IP address and name of the device's address, the vendor's name, the account name, and quantity.

Internal PCI Systems to External

Reports the internal PCI systems that communicate directly with external systems. PCI standards expects that your enterprise can justify this type of traffic. The table provides results by the IP address of the source system, destination system, and the device; the destination port; the protocol used; and the number of events.

Misconfigured Systems

Reports systems with the most misconfiguration events reported in your environment. The table provides results by IP address and name of the misconfigured system, the name of the event, and number of events.

In general, the most common vulnerability in your environment is misconfigured operating systems, frameworks, libraries, and applications. Misconfigurations include missing security patches or updates, incomplete or ad hoc configurations, use of insecure default configurations, poorly configured HTTP headers, and error messages that contain sensitive information.

Network Routing Configuration Changes

Reports the configuration changes to network routing by IP address. The table provides results by the device changed, the type of change, number of events detected, and date of the most recent event.

Personal Firewall Installed

Reports all personal firewalls found in the network. The table lists the IP address and name of the system hosting the personal firewall, as well as the more recent time that the firewall was detected.

Private IP Addresses Disclosure

Reports the RFC1918 IP addresses that communicate with public IP addresses. The table provides results by IP addresses of the source system, destination system, and device; the protocol used; and the number of events.

Software Inventory

Reports the software found by IP address and host name.

Unauthorized Inbound Traffic to Card Holder Data Environment

Reports the system with the most unauthorized traffic. The table provides results by the IP addresses for the device, the source system, and the destination system; the affected port; the protocol used; and number of events.

Unencrypted Administrative Accesses

Reports the accounts that have had unencrypted administrative access events. The table provides results by the IP address and name of the host, the affected account, the port used, affected process, and number of events.

VPN Configuration Changes

Reports changes to the configuration files of VPN devices. The table provides results by the IP address of the VPN, the product and name, the number of events, and the most recent time that the device was changed.

Encryption Transmission – Requirement 4

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [PCI](#) > [PCI Reports](#) > [Requirement 4:Encryption Transmission](#).

Requirement 4 focuses on about managing and maintaining the security of the card holder data when it is transmitted over open or public networks. Malicious users can exploit vulnerabilities in cryptographic hashes and keys, as well as SSL and TLS. For example, the [Heartbleed Bug](#) is a known SSL vulnerability.

Use the following reports to check for vulnerabilities associated with transmitting encrypted data.

Cryptographic Hash Algorithm Related Vulnerabilities

Reports events by host name that indicate potential vulnerabilities related to hash algorithms. All cryptographic hashes that directly use the full output of a Merkle–Damgård construction are vulnerable to length extension attacks. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Public Key Related Vulnerability Detected

Reports flaws found in cryptographic public keys on hosts, as reported by vulnerability scanners in your environment. The table provides results by name of the event, host and IP address, and number of events.

SSL or TLS Vulnerabilities

Reports all SSL and TLS vulnerabilities detected by host name. The table provides results by name of the event, host and IP address, and number of events.

TLS BREACH Vulnerabilities

Reports TLS BREACH vulnerabilities detected by host name. A TLS BREACH attack is a form of the [CRIME attack](#) against HTTP compression. The table provides results by name of the event, host and IP address, and number of events.

TLS CRIME Vulnerabilities

Reports the hosts detected of having vulnerabilities to a TLS CRIME attack. In a CRIME attack, malicious users access the content of secret authentication cookies, so they can hijack sessions of an authenticated web session, then launch additional attacks. The table provides results by name of the event, host and IP address, and number of events.

Wireless Encryption Violations

Reports the hosts that have wireless encryption violations, as detected by vulnerability scanners. The table provides results by name of the event, host and IP address, and number of events.

Track and Monitor Data Access – Requirement 10

Select [Reports](#) > [Portal](#) > [Repository](#) > [Standard Content](#) > [PCI](#) > [PCI Reports](#) > [Requirement 10:Track and Monitor Data Access](#).

To detect and prevent data breaches, you should track changes to user accounts and groups. Malicious users might create groups or accounts to grant them access to sensitive data, then delete their changes to hide their activity.

Account Creation

Reports all user accounts created. The table provides results by IP address and name of the originating system, as well as the name of the new account.

Account Deletion

Reports all user accounts that have been deleted. The table provides results by name of the account that made the change, IP address and name of the host system, and name of the deleted account.

Account Modification

Reports all user accounts that have been modified. The table provides results by the type of modification, name of the changed account, the account that made the change, and the IP address and name of the host system.

User Group Creation

Reports all user groups created. The table provides results by the event, the new user group, and new account name.

User Group Deletion

Reports all user groups deleted. The table provides results by the event, the new user group, and new account name.

VI Using Visuals and Reports to Analyze Data

The **Reports** feature allows you to browse and filter your dataset and to visualize results in a dashboard. Rapidly discover meaningful trends and associations that yield actionable intelligence. Leverage the included MITRE ATT&CK, cloud-based, system, and foundational reports and dashboards to quickly launch [threat-hunting](#) exercises.

Depending on your [assigned permissions](#), you can view, schedule, design, or manage reports and dashboards.

- ♦ [Chapter 18, “Accessing Reports and Dashboards,” on page 139](#)
- ♦ [Chapter 19, “Scheduling Report Generation,” on page 141](#)
- ♦ [Chapter 20, “Designing Dashboards for Data Analysis,” on page 143](#)
- ♦ [Chapter 21, “Designing Reports for Data Analysis,” on page 145](#)
- ♦ [Chapter 22, “Adding and Removing Report Content,” on page 147](#)
- ♦ [Chapter 23, “Best Practices for the Report Designer and Dashboard Designer,” on page 149](#)

18 Accessing Reports and Dashboards

You must have one of the [Reports permissions](#) to use this feature.

Select **Reports** > **Portal**.

The Reports **Portal** provides a repository of built-in reports and dashboards for data analysis, including [MITRE ATT&CK content](#) for use in threat hunting. You [add](#) custom reports and dashboards by collecting and filtering data from your connected sources. The Reports feature supports the ability to drill down into specific elements for thorough data reviews.

The built-in admin reports enable a report administrator track use of the Portal.

19 Scheduling Report Generation

*You must have the **Report Admin** or **Schedule Reports** permission to use this feature.*

Select **Reports** > **Scheduler**.

The Reports **Scheduler** enables you to schedule and manage batch **report** generation. You can create one or more scheduled tasks for which you specify a time condition, reports to be generated, and delivery mechanism of the generated output.

The Reports feature can output the reports in formats such as PDF and Excel. The Scheduler can send the reports in email, save to disk or an archive, or print them.

20 Designing Dashboards for Data Analysis

*You must have the **Report Admin** or **Design Reports** permission to use this feature.*

Select **Reports** > **Dashboard Designer**.

Dashboard Designer provides a wizard that allows you to create new **dashboards** from your data sources. You can dynamically filter a dataset and visualize the output on tables, charts, and gauges. The Designer saves all attributes and related information in a template file in XML format.

The Designer offers you the same functionality as an API, but makes most tasks, such as report layout, much simpler. You can also use the Designer to attach scripts to embed business logic into the report.

21 Designing Reports for Data Analysis

*You must have the **Report Admin** or **Design Reports** permission to use this feature.*

Select **Reports** > **Report Designer**.

Report Designer provides a wizard that allows you to create new [reports](#) from your data sources. You can design elements, change their attributes, and control all aspects of element presentation and layout. The Designer saves all attributes and related information in a template file in XML format. The Designer also supports visually building queries against multiple types of data sources and specifying data grouping, summarization and element data binding.

NOTE: When you create a query in a report, Report Design displays the coding-style name for search fields. For more information, see [Appendix A, “Mapping Database Names to their Appropriate Search Fields,”](#) on page 173.

The Designer offers you the same functionality as an API, but makes most tasks, such as report layout, much simpler. You can also use the Designer to attach scripts to embed business logic into the report.

22 Adding and Removing Report Content

You must have the **Report Admin** permission to use this feature.

Select **Reports > Content**.

The Reports **Content** enables administrators to modify the reports and dashboards in the following ways:

- ♦ [Add and remove content](#), also known as assets, for the reports and dashboards using the **Import Assets** and **Export Assets** feature.
- ♦ [Connect to data sources](#) using the **Add Data Source** feature. Using this feature, you can gather content from specific sources to supply reports and dashboards.

Import and Export Content

Use the **Import Assets** and **Export Assets** options to manage the reports and dashboard available to your users. You can move assets from one server environment to another. For example, you might want to move a set of reports from a test server to a production server.

NOTE: If Reporting generates errors when you attempt to export assets, you should reduce the number of assets that you export concurrently. Alternatively, you might need to increase the RAM for the Reporting node. For more information about sizing your environment for the workload, see the [Technical Requirements for the ArcSight Platform](#).

Supported Data Sources

You can incorporate data from the following sources:

Text/Excel Directory

Connects to a specified file (text or Excel) or file location.

To access and upload this file type, you must create a new folder for your files in the `/var/lib/inetsoft/` path on the reporting server. You might need assistance from your Server Admin.

REST JSON

Connects to a REST (Representational State Transfer) data source containing JSON (JavaScript Object Notation)-formatted data.

REST XML

Connects to a REST data source containing XML-formatted data.

JDBC

Connects to a relational database using Java Database Connectivity.

This source supports commercial and open source databases such as Oracle, SQL Server, DB2, Sybase, Informix, MySQL, PostgreSQL, Vertica, and MS Access. Be sure to download the [latest driver](https://www.inetsoft.com/support/drivers.jsp) (<https://www.inetsoft.com/support/drivers.jsp>).

Elasticsearch REST

Connects to an open source search engine.

NOTE: The process for adding this type of data source is the same as for adding an Elasticsearch data source.

R

Connects to an R database containing R language sources.

23 Best Practices for the Report Designer and Dashboard Designer

When using the Reports module, use these best practices to improve your work flow for creating reports and dashboards.

- ♦ [“Using Search Results to Create a Dashboard or Report” on page 149](#)
- ♦ [“Using Data Models to Build a Worksheet” on page 151](#)
- ♦ [“Using Data Worksheets to Build a Dashboard or Report” on page 151](#)
- ♦ [“Creating a Simple Dashboard” on page 152](#)
- ♦ [“Creating a Simple Scheduled Report” on page 153](#)
- ♦ [“Creating a Simple Report” on page 154](#)

Using Search Results to Create a Dashboard or Report

Each completed search has a unique [Search Results ID](#), which represents a link to the temporary table containing the search results. You can copy that ID, then build a report or dashboard around the search results.

- ♦ [“Build a Report Using Search Results” on page 149](#)
- ♦ [“Build a Dashboard Using Search Results” on page 150](#)
- ♦ [“Convert the Search Fields to Human-Readable Values” on page 150](#)

Build a Report Using Search Results

You can build a report around results of a previously run search by leveraging the [Search Results ID](#).

- 1 When viewing an [Events table](#), select the **Copy** icon in the table’s header.
This icon contains the [Search Results ID](#).
- 2 Select **Reports > Report Designer**.
- 3 Select **Create > Report**.
- 4 In the **Select a data source** field, paste the Search Results ID that you copied.
The retention period of the temporary table in the database is 30 days.
- 5 (Optional) [Convert the fields](#) in the temporary table to human-readable values.
- 6 Continue [creating the report](#).

Build a Dashboard Using Search Results

You can build a dashboard around results of a previously run search by leveraging the [Search Results ID](#).

- 1 When viewing an [Events table](#), select the **Copy** icon in the table's header.
This icon contains the [Search Results ID](#).
- 2 Select **Reports > Dashboard Designer**.
- 3 Select **Create > New Dashboard**.
- 4 From the visual composer, select **Data Source > Database > TABLE > Default_secops_recon**.
- 5 Select the ID of the search that you previously copied.
The retention period of the temporary table in the database is 30 days.
- 6 Select **Open wizard** or **OK**.
- 7 (Optional) [Convert the fields](#) in the temporary table to human-readable values.
- 8 Continue [creating the dashboard](#) where the Search Results ID is the data source.

Convert the Search Fields to Human-Readable Values

The ArcSight Database uses a temporary table to store content associated with a [Search Results ID](#). Because the names of the fields in the table represent the coding-style name, you might want convert the terms to more user-friendly values.

To change the field names, your report or dashboard must use a [Data Worksheet](#).

- 1 Select **Reports > Dashboard Designer**.
- 2 Open the dashboard or report that you want to modify.
- 3 From the upper-right corner, select the **Data** icon.
- 4 Open the [worksheet](#).
- 5 In the lower pane, select the **Formula Editor** icon.
The tool-tip for this icon says "Create Expression."
- 6 Select **SQL**.
- 7 In the Expression pane of the Formula Editor, add the following strings:

```
Time: to_timestamp(field['normalizedEventTime']/1000)
IP:   v6_ntoa(field['sourceAddressBin'])
MAC:  mac_btoa(field['sourceMacAddressBin'])
```
- 8 Select **OK**.
- 9 In the lower pane of the worksheet, select the **Change Data Mode** icon.
- 10 Select **Live Event** data.
- 11 Hide the binary (original) fields.
- 12 **Export** or **Save** the dashboard or report as needed.

Using Data Models to Build a Worksheet

Select **Reports** > **Reports Designer** > **Report type** > **Data Source** > **Database**.

Data models are logical models of the events table in the database that allow for an extra level of abstraction where you can perform varied transformations. You can use the final data model as the final table when creating a [data worksheet](#). By default, the system has two data models:

Basic Data Model

Contains fewer columns from the events table. Use this model for an easier understanding or for simple reports that require less fields.

Event View

Contains the entire events table.

You can also create, edit, and delete your own Data Models. For more information, see “Create a Data Model” in the Help in the Reports Portal. Make sure to add only the fields you that need and create the filters from there. Some of the fields in the data model are non-human readable. You should parse them to ensure that they are readable in the report.

Using Data Worksheets to Build a Dashboard or Report

Data worksheets define the base for the reports and dashboards. Using data worksheets allows you to freely manipulate different data origins and generate a final set of results that can be used for reports and dashboards.

- 1 Select **Reports** > **Dashboard Designer** or **Report Designer**.
- 2 From the upper-right corner, select the **Data** icon.
- 3 From the right corner, select the **New Data Worksheet** icon.
- 4 To start the worksheet, complete one of the following actions:
 - 4a (Conditional) To browse for a data source, select **Database Query**, then **OK**.
 - 4b (Conditional) To import a data file, select **Upload File**, then **OK**.
 - 4c (Conditional) To open a new worksheet then select the data source, select **Mashup Data**, then **OK**.
 - 4d (Conditional) To open a new worksheet, select **Cancel**.
- 5 Drag and drop the fields, tables, or queries that you want to include in the dashboard or report. Alternatively, you can create tables, then link them using unions or joins.
- 6 (Conditional) To refine the design, select one of the following options from the **Preview** pane. For example, you can sort and reorder the columns or change the data mode.
- 7 To save your changes, complete the following steps:
 - 7a Select **Save** or **Save As**.
 - 7b Specify the folder where you want to save the worksheet.

Do not specify the **Standard Content** folder, which is reserved for the built-in reports and dashboards.
- 8 Exit the Data Worksheet as needed.

Creating a Simple Dashboard

When creating a simple dashboard, Reports prompts you to select the data source. When you open the Dashboard Visual Composer, a window displays where you can choose the data source for the Dashboard. Follow the prompts or close the window to continue to the main editor of the Dashboard.

From the Dashboard editor, you can create Tables and Charts in the canvas. From there, you can also convert to measure some fields that can provide numeric values and can be used in a chart. You can also convert to dimension the fields that can provide a string value.

First, use the system to create and save a [data worksheet](#) as the basis for your dashboard. Use one of the following to create a simple dashboard.

- ♦ [“Use the Dashboard Wizard” on page 152](#)
- ♦ [“Use the Dashboard Editor” on page 152](#)

Use the Dashboard Wizard

If you select the wizard, the Dashboard Designer displays the Wizard section of the Dashboard. From here, you can create the first component of the Dashboard.

- 1 Select **Reports > Dashboard Designer > Crosstab Wizard**.
- 2 Select the **data worksheet** of your preference as a data source, and click **Next**.
- 3 Select **Open Wizard**.
- 4 Select the fields to use in your dashboard.
- 5 (Conditional) Select the dashboard style.
 - 5a Crosstab: Groups the dashboard by row and column headers and displays the summary data at the intersections.
 - 5b Table: Groups the dashboard and summarizes it or displays it in tabular layout.
 - Chart: Creates multiple charts using multiple fields.
 - Full Editor: Allows granular control view of your updates, such as format, color, and shape.
- 6 Once the editing is complete, set the position of the element in the dashboard canvas.
- 7 View the dashboard, then select **Continue**.
- 8 Once the dashboard has been successfully edited, select **Finish**.
- 9 Click **Save as** to save your dashboard.

Use the Dashboard Editor

Using the Dashboard Designer, you can edit the elements and freely set their position in the Dashboard. The Dashboard Designer displays the Wizard section of the Dashboard.

- 1 Select **Reports > Dashboard Designer > Crosstab Wizard**.
- 2 Click **Cancel** to open the dashboard editor.
- 3 Select the **data worksheet** of your preference as a data source, and click **Next**.
- 4 Add the elements available from the left.

- 5 Update the dashboard using the Dashboard composer. You can create, add, and edit multiple elements.
- 6 Click **Save** to save your dashboard in a **Custom Content** folder.

Creating a Simple Scheduled Report

You can create a report that runs on your chosen schedule. In the report, define conditions that trigger tasks and actions you want to run.

- 1 Select **Reports > Scheduler**.
- 2 In the lower left corner of the screen, select **New Task**.
- 3 For **Name**, enter a name of the task.
- 4 To set the conditions for your report, complete the following steps:
 - 4a Select the **Condition** tab.
 - 4b (Conditional) To specify the timezone that the report uses, perform one of the following actions:
 - ♦ To use the timezone where the server is installed, select **Show Server Time Zone**
 - ♦ To use your timezone, deselect **Show Server Time Zone**
 - 4c (Conditional) To run the task at specific intervals, configure the frequency.
For example, to run a report every Monday afternoon, specify the following settings:
 - ♦ Select **Time Range**, then **Afternoon**.
 - ♦ For **Every**, enter 1
 - ♦ Select **Monday**.
 - 4d (Conditional) To run the tasks in sequence, select **Chained**, then specify the first task.
 - 4e Select **OK** to save the scheduled task.
- 5 To specify the report associated with the scheduled tasks, complete the following steps:
 - 5a Select the **Action** tab.
 - 5b For **Report**, click **Select** then navigate to the report that you want to schedule.
 - 5c To email the report results, select **Deliver to Emails** then configure the email content and destination addresses.
 - 5d To set the time range in which the report retrieves data, complete one of the following actions:
 - ♦ Select **Add**, then specify the time values.
 - ♦ Select **Creation Parameters**, then choose the dates from the calendar option.
 - 5e Select **OK** to save your changes.

Creating a Simple Report

First, create and save a data worksheet. For additional details on how to create a data worksheet, see [Using Data Worksheets to Build a Dashboard or Report](#).

Use the one of the following wizards to create a simple report.

- ♦ [“Use the Crosstab Wizard” on page 154](#)
- ♦ [“Use the Table Wizard” on page 154](#)
- ♦ [“Use the Chart Wizard” on page 155](#)
- ♦ [“Guidelines for Report Usage” on page 155](#)

Use the Crosstab Wizard

From the Reports Designer menu, use the Crosstab Wizard to create a report that displays data in a pivot table where the data is grouped by row and column headers, and the summary data is displayed at the intersections.

- 1 Select **Reports > Report Designer > Crosstab Wizard**.
- 2 Select the **data worksheet** of your preference as a data source, and click **Next**.
- 3 Define the **row and column groups** (vertical and horizontal columns), and click **Next**.
 - 3a Row groups: Select the row headers.
 - 3b Column groups: Select the column headers.
- 4 (Conditional) Define the **summary columns** that will display as summarized fields.
- 5 (Conditional) **Filter the conditions** that will define the original data. After the design statement is filled, the options for insert, modify, and clear will be enabled.
- 6 (Conditional) For **table style**, use the default option.
- 7 To complete the editing, click **Finish Editing**.

Use the Table Wizard

From the Reports Designer menu, use the Table Wizard to create a report that displays data in tabular layout or grouped and summarized.

- 1 Select **Reports > Report Designer > Table Wizard**.
- 2 Select the **data worksheet** of your preference as a **data source**.
- 3 Select the columns to display in the report from the select **detail columns**.
- 4 Define the groups to display as **column headers**.
- 5 (Conditional) Define the **summary columns** that will display as summarized fields.
- 6 (Conditional) Filter the conditions to define the original data. Once the design statement is filled, the control options are enabled.
- 7 (Conditional) Retain the default **table style** for better formatting results.
- 8 (Conditional) Rank the groups to display as top or bottom groups.

Use the Chart Wizard

From the Reports Designer menu, use the Chart Wizard to create a chart-based report.

- 1 Select **Reports > Report Designer > Chart Wizard**.
- 2 Select the data worksheet of your preference as a data source.
- 3 By default, the auto option is selected. Use the **chart style** to style your report.
- 4 (Conditional) If required, select one of the following 2D and 3D images chart styles: Bar, line, area, point, pie, donut, radar, stock, candle, box plot, waterfall, pareto, map, treemap, and marimeko.
- 5 Define the **X Axis** that to display as columns.
- 6 Define the **Y Axis** to display as columns.
- 7 Define the visual properties (color, shape, size, text) of the columns by using the visual binding.
- 8 (Conditional) Filter the conditions to define the original data. Once the design statement is filled, the control options are enabled.
(Conditional) Rank the groups to display as top or bottom groups.
- 9 (Conditional) Additional steps might be required depending on the chart style selected.

Geographic binding

Use if you select **Map Style** for your report. Choose different aspects about the map report that will be generated.

Tree dimensions

Use if you select **Treemap**, **Sunburst**, **Circle Packing**, or **Icicle** for your report. Select the fields the report will use for the Tree Mapping.

Marimekko category

Use if you select **Marimekko Style** for your report. Select the field for the Marimekko Category Dimension.

Guidelines for Report Usage

- ♦ Create as many data models as needed but only include the fields that you need for your report.
- ♦ Use the Basic Data Model instead of the event view for simple reports.
- ♦ To convert non-human readable fields in the data model, parse them prior adding them to the report.
- ♦ You can create filters from the data model or the report itself. It is recommended to set the filters from the data model so these can be saved in the data base.
- ♦ Check the meta data box for a faster pre-visualization of the report. Take into consideration that no real data is displayed with this option.
- ♦ Export the results in CSV format for faster results.
- ♦ When needed, copy the bundled dashboards from the Recon Installation and use them as templates for other creations.

VII

Managing Your Stored Data

*You must have the **Manage Storage Groups** permission to use this feature.*

Search performance can be affected by your environment's set up and the way that your data is organized. To enable faster search times, you can configure Recon to organize data into [storage groups](#), which represent partitions in the ArcSight database. These storage groups can support compliance requirements for data retention policies, such as those for the Payment Card Industry Data Security Standard (PCI DSS). For example, you might be required to retain certain data for 12 to 24 months. You can instruct Recon to [purge](#) data that is older than a certain number of months. By deleting data, you reduce the amount of content within the database and improve search performance.

- ♦ [Chapter 24, "Organizing Your Data," on page 159](#)

24 Organizing Your Data

You must have the **Manage Storage Groups** permission to use this feature.

Select **Configuration > Storage**.

The **Storage Information** list provides an overview of all available [storage groups](#). You can have up to 10 storage groups, each with specific retention periods and query filters. To find a storage group, use the **Search** field.

- ♦ [“Use Storage Groups to Organize and Retain Data” on page 159](#)
- ♦ [“Activate and Deactivate Storage Groups” on page 160](#)
- ♦ [“Change the Settings of a Storage Group” on page 161](#)
- ♦ [“Set Retention Policies for the Data” on page 162](#)
- ♦ [“Use Storage Group Queries in a Search” on page 162](#)

Use Storage Groups to Organize and Retain Data

Recon can divide data into **storage groups**, which allows you to partition the incoming events data and provide different retention periods, based on the query filter. Because you can set [data retention policies](#) per storage group, you can retain certain high volume events for a short time period and other important events for longer time period.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Recon uses the specified query filters to [direct events](#) to the correct storage group. For example, one group might have a filter for `categoryDeviceGroup =/ Firewall` and another for `severity >= 7`. If an event does not match any of the active filters, Recon sends the event to the *Default Storage Group*. You cannot change the name, query, or rank of this built-in group.

Recon displays a **Apply Changes to System** option at the top of the Storage Groups page to let you know that one or more groups have been modified but the [changes need to be applied](#) yet.

- ♦ [“Create a Storage Group” on page 159](#)
- ♦ [“Direct Events to the Correct Storage Group” on page 160](#)

Create a Storage Group

Recon allows you to have up to **10 storage groups**, including the provided *Default Storage Group*.

- 1 Select **Configuration > Storage**.
- 2 Select +.

- 3 Enter a name for the storage group.

IMPORTANT: You cannot change the name after you create the group. Also, the name cannot include special characters.

- 4 Enter a query with which to filter the incoming events into this storage group.
For example, `categoryDeviceGroup='/Firewall'` or `categoryDeviceGroup='/IDS'`.
The query can include parentheses, quotes, and single quotes.
- 5 For the storage group's status, indicate whether to [activate the group](#).
- 6 (Optional) For **Delete Data Older than**, enter the age of data, in months, that you want to [purge](#) from the storage group in the database.
- 7 Select **SAVE**.
- 8 [Apply your changes](#).

Direct Events to the Correct Storage Group

For efficient data retrieval, Recon matches each incoming event with the query filter for single, active storage group. However, an event could be associated with the rules of more than one group. When an event matches with multiple storage groups, Recon **assigns the event to the highest ranked group**. For example, if *Event_29* matches the query filter for the storage groups ranked 3, 5, and 6, then Recon assigns the event to the group that is ranked 3. If an event does not match any of the active filters, Recon sends the event to the *Default Storage Group*.


You can change the ranking of storage groups to ensure that Recon places events in the best location.

- 1 Select **Configuration > Storage**.
- 2 In the **Storage Information** list, drag each storage group up or down to the preferred priority position.
Recon always places the *Default Storage Group* in the lowest ranked position.

Activate and Deactivate Storage Groups

Recon allows you to have up to **10 storage groups**, including the provided *Default Storage Group*. To inactive to prevent new events from being sent to the group, change a storage group's status. For example, you might no longer need a particular storage group or find that you have changed the filters and functionality of that group from its original purpose. Rather than continuing to modify an existing group, you can deactivate it. Alternatively, you might want to activate a storage group only during certain periods of time.

Although you deactivate a group, the [deletion](#) settings for that group remain in effect.

- 1 Select **Configuration > Storage**.
- 2 Select the storage group that you want to activate or deactivate.
- 3 Select .
- 4 For **Group Status**, slide the indicator left or right.

Activated groups will display a status of **Active**.

- 5 Select **SAVE**.


Change the Settings of a Storage Group

After [creating](#) or [modifying](#) storage groups, you must [apply](#) the changes. You can modify multiple groups before applying your changes.

- ♦ [“Modify a Storage Group” on page 161](#)
- ♦ [“Apply Your Changes to a Storage Group” on page 161](#)

Modify a Storage Group

You can modify a storage group at any time.

- 1 Select **Configuration** > **Storage**.
- 2 Select the storage group that you want to modify.
- 3 Select .
- 4 For **Group Status**, slide the indicator left or right.
Activated groups will display a status of **Active**.
- 5 Select **SAVE**.
- 6 [Apply your changes](#).

Apply Your Changes to a Storage Group

Select **Configuration** > **Storage** > **Apply Changes to System**.

When you change the query filter, [status](#), or [rank](#) of a storage group, your changes do not go into effect until you apply the changes. The following considerations affect how your changes are applied:

- ♦ If you modify the query filter, Recon will begin adding events that match the updated filter. However, the storage group retains all currently stored events associated with the previous filter. The retention policies continue to apply to all events within the group.

If you do not want the storage group to have both sets of events, you can create a new storage group for the updated query filter, then [deactivate](#) the older storage group.

- ♦ On the first day of the month, Recon deletes events matching the [retention policies](#) of the storage groups. For example, on March 15, you change the deletion time to three months from four months. On April 1, Recon begins deleting all data older than three months.
- ♦ While changes are being applied, you cannot create or modify a storage group.

Set Retention Policies for the Data

The Watchdog service in the database monitors system storage capacity. If the capacity exceeds a certain threshold then Watchdog tells the database to start deleting the oldest partitions until disk usage drops below the threshold. By default, the Watchdog threshold is 95% of capacity. To prevent the purging of needed data, you can use storage groups to set retention policies for [deleting](#) specific data.

When setting the policies for storage group retention and disk space utilization, do not allow your storage group utilization to increase above 90%. As storage groups near 99% utilization, they start running out of disk space, which reduces the performance of searches due to increasing fragmentation.

- ♦ [“Delete Old Data” on page 162](#)

For more information about Watchdog, see the [Administrator’s Guide to ArcSight Platform](#) on the ArcSight documentation site.

Delete Old Data

Events are stored in their assigned storage groups either in the ArcSight database. Over time, the storage system can retain unneeded or outdated data. To preserve space in the database and improve data retrieval from storage groups, you can configure the database to remove events older than a certain number of months. For example, your data retention policy might expect data older than 24 months to be purged. This process **deletes data from the database**.

Search automatically applies all deletion settings on the first day of the month at 2:10 a.m.

- 1 [Create](#) or [modify](#) a storage group.
- 2 For **Delete Data Older than**, enter the age of data, in months, that you want to be deleted.
Ensure that your retention policy takes into consideration the maximum size of your storage groups and database. If a storage group fills up, the oldest events could be purged automatically to make room for incoming events, even if the older events are within the retention period.
- 3 Select **SAVE**.
- 4 [Apply your changes](#).

Use Storage Group Queries in a Search

Search allows you to include a storage group in a query. Rather than entering the query filter of a storage group again in Search, [specify](#) the following for your Search query: `Storage Group = Firewall Events`. By specifying the storage group, you limit the search to that storage group’s partitions only, thus improving search performance.

VIII Managing User Access and Preferences

The Fusion capability in the ArcSight Platform supports user management, where you can add users, create roles, and assign roles. Recon adds a [role](#) and several [permissions](#) to the common set of roles and permissions available with Fusion. As a user, you can specify the settings that you [prefer to use](#) for all searches.

- ♦ [Chapter 25, “Assigning Permissions for Recon,” on page 165](#)
- ♦ [Chapter 26, “Default Roles for Recon,” on page 167](#)
- ♦ [Chapter 27, “Configuring User Preferences,” on page 169](#)

25 Assigning Permissions for Recon

To view your permissions, select **your_ID** > *My Profile* > **Permissions**.

To assign permissions to a **role**, select **ADMIN** > **Roles**.

Recon includes specific permissions for accessing or managing the following activities:

- ♦ Using [Search](#)
- ♦ Running and developing [reports](#)
- ♦ Managing [storage groups](#)
- ♦ Monitoring the database with widgets in the Dashboard

For more information about these permissions or assigning them to a role, select **ADMIN** > **Help** or see the [User Guide for Fusion in the ArcSight Platform](#).

26 Default Roles for Recon

Select **ADMIN** > **Roles**.

When you deploy Recon, Fusion adds Recon's [permissions](#) to the default roles:

- ♦ System Admin
- ♦ Admin
- ♦ Analyst L1
- ♦ Guest
- ♦ User

Fusion also adds a default role to support the [Reports](#) portal: the Report User role.

For more information about assigning these roles, select **ADMIN** > **Help** or see the [User Guide for Fusion in the ArcSight Platform](#).

27 Configuring User Preferences

Select [\[your_ID\]> My Profile > Preferences](#).

Some deployed capabilities enable you to configure preferences for commonly used settings. For example, in Recon, if you regularly use the same fieldset for a Search, you can specify that set as your preferred default.

- ♦ [“Configure Search Preferences” on page 169](#)

Configure Search Preferences

Available only when ArcSight Recon is deployed in your environment

To reduce the time required to create and manage searches, configure Search to use your preferred settings. You can always override your preferences as needed when you create a search. When you modify your Search preferences, the changes apply to new searches. Existing searches are not affected unless you re-run the search.

Default Fieldset

Specifies the [fieldset](#) you regularly use for a search. The default value is *Base Event Fields*.

Default View

Specifies if the [Events Table](#) displays results in the [Grid View](#) or [Raw View](#). The default value is *Grid View*.

Time Zone

Instructs Search to adjust the timestamp for events to the chosen [time zone](#).

Date/Time Format

Specifies the format of dates and times you want Search to use. The default is *YYYY/MM/DD*.

Default Time Setting

Specifies the [time range](#) you want Search to find events. The default is *Last 30 minutes*.

Base Searches On

Specifies the [timestamp](#) Recon associates with the event you want to find.

Search Expires In

Specifies how often you want searches to expire, and thus Recon to remove them from the system. Alternatively, you can choose to never remove a search.

Also, the expiration date resets whenever you access the search. Resetting the date includes resuming or re-running the search, as well as saving the search.

Maximum Search Results

Specifies the maximum number of events Search returns. Search considers a search complete when the results reach the maximum limit.

Highlight Query Syntax

Specifies whether Search uses color to differentiate the syntax terms from the operators and functions within the query.

IX Appendices

The appendices in this guide provide additional information or guidance for using the features and functions for this product.

- ♦ [Appendix A, “Mapping Database Names to their Appropriate Search Fields,” on page 173](#)

A Mapping Database Names to their Appropriate Search Fields

When creating a [fieldset](#), Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a [query](#). For example, in a query you can enter or select Agent Address. However, in the fieldsets selection, this same field appears as agentAddressBin. This issue also occurs when you're adding queries to a [Report](#).

The following tables provide the coding-style names that appear in the fieldset and report configurations, so that you can easily map them to their human-readable names.

- ♦ [“Agent Fields” on page 173](#)
- ♦ [“Category Fields” on page 174](#)
- ♦ [“Correlation Fields” on page 174](#)
- ♦ [“Destination Fields” on page 175](#)
- ♦ [“Device Fields” on page 176](#)
- ♦ [“Device Custom Fields” on page 177](#)
- ♦ [“Event Fields” on page 178](#)
- ♦ [“Extension Fields” on page 179](#)
- ♦ [“File Fields” on page 179](#)
- ♦ [“Flex Fields” on page 179](#)
- ♦ [“OldField Fields” on page 180](#)
- ♦ [“Old File Fields” on page 180](#)
- ♦ [“Request Fields” on page 180](#)
- ♦ [“Source Fields” on page 181](#)

Agent Fields

Substitute the following labels in the agent category:

For the field that you want to add...	You should choose...
Agent Address	agentAddressBin
Agent DNS Domain	agentDnsDomain
Agent Hostname	agentHostName
Agent ID	agentId
Agent Mac Address	agentMacAddressBin
Agent NT Domain	agentNtDomain

For the field that you want to add...	You should choose...
Agent Receipt Time	agentReceiptTime
Agent Severity	agentSeverity
Agent Timezone	agentTimeZone
Agent Translated Address	agentTranslatedAddressBin
Agent Translated Zone External ID	agentTranslatedZoneExternalID
Agent Translated Zone URI	agentTranslatedZoneURI
Agent Type	agentType
Agent Version	agentVersion
Agent Zone External ID	agentZoneExternalID
Agent Zone URI	agentZoneURI

Category Fields

Substitute the following labels in the `category` category:

For the field that you want to add...	You should choose...
Category Behavior	categoryBehavior
Category Device Group	categoryDeviceGroup
Category Device Type	categoryDeviceType
Category Object	categoryObject
Category Outcome	categoryOutcome
Category Significance	categorySignificance
Category Technique	categoryTechnique
Version	version

Correlation Fields

Substitute the following labels in the `correlation` category:

For the field that you want to add...	You should choose...
Base Event Ids	correlated_event_id
Correlated Event Id	generatorURI
Generator External ID	generatorExternalID
Generator URI	base_event_ids

For the field that you want to add...	You should choose...
Priority	priority

Destination Fields

Substitute the following labels in the `destination` category:

For the field that you want to add...	You should choose...
Destination Address	destinationAddressBin
Destination DNS Domain	destinationDnsDomain
Destination Geo Country Code	destinationGeoCountryCod
Destination Geo Latitude	destinationGeoLatitude
Destination Geo Longitude	destinationGeoLongitude
Destination Geo Postal Code	destinationGeoPostalCode
Destination Geo Region Code	destinationGeoRegionCode
Destination Geolocation Info	destinationGeoLocationInfo
Destination Hostname	destinationHostName
Destination Mac Address	destinationMacAddressBin
Destination NT Domain	destinationNtDomain
Destination Port	destinationPort
Destination Process ID	destinationProcessId
Destination Process Name	destinationProcessName
Destination Service Name	destinationServiceName
Destination Translated Address	destinationTranslatedAddressBin
Destination Translated Port	destinationTranslatedPort
Destination Translated Zone External ID	destinationTranslatedZoneExternalID
Destination Translated Zone URI	destinationTranslatedZoneURI
Destination User ID	destinationUserId
Destination User Privileges	destinationUser Privileges
Destination Username	destinationUserName
Destination Zone External ID	destinationZoneExternalID
Destination Zone URI	destinationZoneURI

Device Fields

Substitute the following labels in the `device` category:

For the field that you want to add...	You should choose...
Device Action	<code>deviceAction</code>
Device Address	<code>deviceAddressBin</code>
Device Asset ID	<code>deviceAssetID</code>
Device Direction	<code>deviceDirection</code>
Device DNS Domain	<code>deviceDnsDomain</code>
Device Domain	<code>deviceDomain</code>
Device Event Category	<code>deviceEventCategory</code>
Device Event Class ID	<code>deviceEventClassId</code>
Device External ID	<code>deviceExternalId</code>
Device Facility	<code>deviceFacility</code>
Device Hostname	<code>deviceHostName</code>
Device Inbound Interface	<code>deviceInboundInterface</code>
Device Mac Address	<code>deviceMacAddressBin</code>
Device NT Domain	<code>deviceNtDomain</code>
Device Outbound Interface	<code>deviceOutboundInterface</code>
Device Process ID	<code>deviceProcessId</code>
Device Process Name	<code>deviceProcessName</code>
Device Product	<code>deviceProduct</code>
Device Receipt Time	<code>deviceReceiptTime</code>
Device Severity	<code>deviceSeverity</code>
Device Timezone	<code>deviceTimeZone</code>
Device Translated Address	<code>deviceTranslatedAddressBin</code>
Device Translated Zone External ID	<code>deviceTranslatedZoneExternalID</code>
Device Translated Zone URI	<code>deviceTranslatedZoneURI</code>
Device Vendor	<code>deviceVendor</code>
Device Version	<code>deviceVersion</code>
Device Zone External ID	<code>deviceZoneExternalID</code>
Device Zone URI	<code>deviceZoneURI</code>
Normalized Event Time	<code>normalizedEventTime</code>

Device Custom Fields

Substitute the following labels in the `device custom` category:

For the field that you want to add...	You should choose...
Device Custom Date 1	<code>deviceCustomDate1</code>
Device Custom Date 1 Label	<code>deviceCustomDate1Label</code>
Device Custom Date 2	<code>deviceCustomDate2</code>
Device Custom Date 2 Label	<code>deviceCustomDate2Label</code>
Device Custom Descriptor ID	<code>deviceCustomDescriptorId</code>
Device Custom Floating Point 1	<code>deviceCustomFloatingPoint1</code>
Device Custom Floating Point 1 Label	<code>deviceCustomFloatingPoint1Label</code>
Device Custom Floating Point 2	<code>deviceCustomFloatingPoint2</code>
Device Custom Floating Point 2 Label	<code>deviceCustomFloatingPoint2Label</code>
Device Custom Floating Point 3	<code>deviceCustomFloatingPoint3</code>
Device Custom Floating Point 3 Label	<code>deviceCustomFloatingPoint3Label</code>
Device Custom Floating Point 4	<code>deviceCustomFloatingPoint4</code>
Device Custom Floating Point 4 Label	<code>deviceCustomFloatingPoint4Label</code>
Device Custom Number 1	<code>deviceCustomNumber1</code>
Device Custom Number 1 Label	<code>deviceCustomNumber1Label</code>
Device Custom Number 2	<code>deviceCustomNumber2</code>
Device Custom Number 2 Label	<code>deviceCustomNumber2Label</code>
Device Custom Number 3	<code>deviceCustomNumber3</code>
Device Custom Number 3 Label	<code>deviceCustomNumber3Label</code>
Device Custom String 1	<code>deviceCustomString1</code>
Device Custom String 1 Label	<code>deviceCustomString1Label</code>
Device Custom String 2	<code>deviceCustomString2</code>
Device Custom String 2 Label	<code>deviceCustomString2Label</code>
Device Custom String 3	<code>deviceCustomString3</code>
Device Custom String 3 Label	<code>deviceCustomString3Label</code>
Device Custom String 4	<code>deviceCustomString4</code>
Device Custom String 4 Label	<code>deviceCustomString4Label</code>
Device Custom String 5	<code>deviceCustomString5</code>
Device Custom String 5 Label	<code>deviceCustomString5Label</code>

For the field that you want to add...	You should choose...
Device Custom String 6	deviceCustomString6
Device Custom String 16 Label	deviceCustomString6Label
Device CustomIPv6 Address 1	deviceCustomIPv6Address1Bin
Device CustomIPv6 Address 1 Label	deviceCustomIPv6Address1Label
Device CustomIPv6 Address 2	deviceCustomIPv6Address2Bin
Device CustomIPv6 Address 2 Label	deviceCustomIPv6Address2Label
Device CustomIPv6 Address 3	deviceCustomIPv6Address3Bin
Device CustomIPv6 Address 3 Label	deviceCustomIPv6Address3Label
Device CustomIPv6 Address 4	deviceCustomIPv6Address4Bin
Device CustomIPv6 Address 4 Label	deviceCustomIPv6Address4Label

Event Fields

Substitute the following labels in the `event` category:

For the field that you want to add...	You should choose...
Application Protocol	applicationProtocol
Base Event Count	baseEventCount
Bytes In	bytesIn
Bytes Out	bytesOut
Crypto Signature	cryptoSignature
Customer External ID	customeExternalID
Customer URI	customerURI
End Time	endTime
Event ID	eventId
Event Outcome	eventOutcome
External Id	externalID
Locality	locality
Message	message
Name	name
Originator	originator
Reason	reason
Start Time	startTime

For the field that you want to add...	You should choose...
Transport Protocol	transportProtocol
Type	type

Extension Fields

Substitute the following labels in the `extension` category:

For the field that you want to add...	You should choose...
Extra Fields	extraFields
Storage Group	storageGroup

File Fields

Substitute the following labels in the `file` category:

For the field that you want to add...	You should choose...
File Create Time	fileCreateTime
File Hash	fileHash
File ID	fileId
File Modification Time	fileModificationTime
File Name	fileName
File Path	filePath
File Permission	filePermission
File Size	fileSize
File Type	fileType

Flex Fields

Substitute the following labels in the `flex` category:

For the field that you want to add...	You should choose...
Flex Date 1	flexDate1
Flex Date 1 Label	flexDate1Label
Flex Number 1	flexNumber1
Flex Number 1 Label	flexNumber1Label

For the field that you want to add...	You should choose...
Flex Number 2	flexNumber2
Flex Number 2 Label	flexNumber2Label
Flex String 1	flexString1
Flex String 1 Label	flexString1Label
Flex String 2	flexString2
Flex String 2 Label	flexString2Label

OldField Fields

Substitute the following labels in the `oldfield` category:

For the field that you want to add...	You should choose...
Old File Create Time	oldFileCreateTime

Old File Fields

Substitute the following labels in the `old file` category:

For the field that you want to add...	You should choose...
Old File Hash	oldFileHash
Old File ID	oldFileId
Old File Modification Time	oldFileModificationTime
Old File Name	oldFileName
Old File Path	oldFilePath
Old File Permission	oldFilePermission
Old File Size	oldFileSize
Old File Type	oldFileType

Request Fields

Substitute the following labels in the `request` category:

For the field that you want to add...	You should choose...
Request Client Application	requestClientApplication
Request Context	requestContext

For the field that you want to add...	You should choose...
Request Cookies	requestCookies
Request Method	requestMethod
Request URL	requestUrl
Request URL FileName	requestUrlFileName
Request URL Query	requestUrlQuery

Source Fields

Substitute the following labels in the `source` category:

For the field that you want to add...	You should choose...
Source Address	sourceAddressBin
Source DNS Domain	sourceDnsDomain
Source Geo Country Code	sourceGeoCountryCode
Source Geo Latitude	sourceGeoLatitude
Source Geo Longitude	sourceGeoLongitude
Source Geo Postal Code	sourceGeoPostalCode
Source Geo Region Code	sourceGeoRegionCode
Source Geolocation Info	sourceGeoLocationinfo
Source Hostname	sourceHostName
Source Mac Address	sourceMacAddressBin
Source NT Domain	sourceNtDomain
Source Port	sourcePort
Source Process ID	sourceProcessId
Source Process Name	sourceProcessName
Source Service Name	sourceServiceName
Source Translated Address	sourceTranslatedAddressBin
Source Translated Port	sourceTranslatedPort
Source Translated Zone External ID	sourceTranslatedZoneExternalID
Source Translated Zone URI	sourceTranslatedZoneURI
Source User ID	sourceUserId
Source User Privileges	sourceUserPrivileges
Source Username	sourceUserName

For the field that you want to add...	You should choose...
Source Zone External ID	sourceZoneExternalID
Source Zone URI	sourceZoneURI