# ArcSight Recon 1.1

## User Guide

**December 2020**

## Copyright Notice

# Contents

# 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
- 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 the ArcSight Platform*, which provides information about deploying, configuring, and maintaining the products that you deploy in the containerized environment
- *Technical Requirements for the 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, “Understanding the Search Parameters,” on page 23

# 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.

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.

## Understanding the Search Feature

Recon ingests log data from SmartConnectors routed through ArcSight Transformation Hub. 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 that 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 which timestamp you want 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.

# 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.

# 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**.

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 that you want for the search results.

By default, Search displays the name of the last used 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 that you want to use for the retrieved events. Search uses Normalized Event Time by default.
6. Select **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.

# 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*.

# 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 18
- "View the Events Table" on page 18
- "View and Use the Details of an Event" on page 20
- "Identify Fields without Data" on page 20
- "Refresh Search Results" on page 20

## 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**, 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 that is 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, then deselect 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 20
- "Apply Event Details to Other Searches or Share with Colleagues" on page 20

## 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, `name=''`) | name = ‘’, 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.

# 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.

# 3 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 23
- "Understand the Query Syntax, Operators, and Functions" on page 24
- "Specify a Group of Fields" on page 35
- "Specify an Alias for a Field" on page 35
- "Specify IP Addresses and Subnets" on page 39
- "Include a Storage Group's Filter in the Search Query" on page 40
- "Extend the Search with a Lookup List" on page 40
- "Use Specific Sets of Fields for Search Results" on page 43
- "Configure the Time Range" on page 44
- "Configure Preferred Settings for Searches" on page 46

## 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 then select the criteria that you want 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 |
| #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 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*> |
| #Firewall Events | categoryDeviceGroup = /Firewall |
| #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 |
| #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 |
| #Windows Account Creation | deviceVendor = Microsoft AND deviceEventClassId = Microsoft-Windows-Security-Auditing:4720, Security:624 |

# 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 25
- "Understand the Search Query Functions and Operators" on page 27
- "Understand the Functions for Building Eval Expressions" on page 29

## 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 the ArcSight Platform*.

| Type | Full-text | Field-based | Hashtag (predefined) |
|---|---|---|---|
| Case sensitivity | Case-sensitive | Case-sensitive | Case-insensitive |
| Exact Match | Keyword treated as keyword*.<br>Example:<br>/Execute matches: /Execute, /Execute/Start, /Execute/Response,/Execute/Query | Enclose value in double quotes.<br>Example:<br>`Category Behavior ="/Execute"` | n/a |
| Nesting, including parenthetical clauses, such as (a OR b) AND c | Allowed<br>Use Boolean operators to connect and nest keywords. | Allowed<br>Use Boolean operators to connect and nest keywords. | Allowed<br>Use Boolean operators to connect and nest keywords |

| Type | Full-text | Field-based | Hashtag (predefined) |
|---|---|---|---|
| Implicit Operators | When you enter two values separated by a space, this is treated as an implicit AND condition.<br>Example: `ssh fail` | The AND/OR treatment depends on the operator used in the search.<br>For example, `destinationAddress = 1.1.1.1, 2.2.2.2` is equivalent to `destinationAddress = 1.1.1.1 or destinationAddress = 2.2.2.2,`<br>while the query `destinationAddress != 1.1.1.1, 2.2.2.2` is equivalent to `destinationAddress != 1.1.1.1 and destinationAddress != 2.2.2.2` | n/a |
| List Operations | n/a | Performs an inner join or a left join against a custom list.<br>*Syntax for an Inner Join:* `source address in list CustomListName_CustomColumn Name`<br>*Syntax for a Left Join:* `source address not in list CustomListName_CustomColumnName` | n/a |
| Time Format<br>(when searching for events that occurred at a particular time) | No specific format<br>The query needs to contain the exact timestamp string.<br>Example: "`10:34:35`" | YYYY-MM-DD<br>YYYY-MM-DD HH:mm<br>YYYY-MM-DD HH:mm:ss.fff<br>To narrow the time range, use the following operators:<br>◆ in between (><)<br>◆ greater than (>)<br>◆ less than (<) | n/a |

| Type | Full-text | Field-based | Hashtag (predefined) |
|---|---|---|---|
| Special Characters:<br>\ * ' " | Use the backslash (\) as an escape character. | Use the backslash (\) as an escape character. | n/a |
| Wildcard | Can appear anywhere in the value.<br>Examples:<br>*log<br>log*<br>lo*g*<br>Searches for ablog, blog, long, etc. | Can appear anywhere in the field.<br>Examples:<br>name=*log<br>Searches for ablog, blog, etc. in name field<br>name="*log"<br>name=*log<br>Both search for *log | n/a |
| Escape a Wildcard Character | Can search for * by escaping the character.<br>Example:<br>log* | Can search for * by escaping the character.<br>Example:<br>name=log* | 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<br>sourceAddress equals 10.0.112.9 and destinationAddress = 10.0.116.148 |
| OR | | fail OR ssh<br>destinationAddress = 10.0.111.5 OR destinationAddress=10.0.116.148 destinationAddress =10.0.111.5, 10.0.116.48 |
| not equal | <><br>!= | destinationPort not equal 21 |
| equals | =<br>==<br>is equal to<br>equal | name equals INVALID password<br>device vendor equals CISCO |
| greater than | ><br>is greater | bytes In greater than 100 |

| Operator | Alternative Operator | Examples |
|---|---|---|
| less than | <<br>is less<br>is lower<br>less | bytes out less than 1000 |
| greater equal than | >=<br>gte<br>greater equal | End Time greater equal than 2017-07-25<br>End Time greater equal than 2017-07-25 09:07<br>End Time greater equal than 2017-07-25 09:07:43<br>End Time greater equal than 2017-07-25 09:31:22.685 |
| less equal than | <=<br>lte<br>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<br>like<br>has substring | name contains TCP |
| does not contain | does not have | name does not contain TCP |
| in list | match<br>in list of | device vendor equals CISCO and source address in list customListName_customColumnName<br>device vendor equals CISCO and source address in list badGuyIpList_badGuyIp |
| not in list | not match<br>not in list of | source address not in list customListName_customColumnName<br>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 |
| \|<br>(Pipeline operator) | n/a | Combine various search functions separated by the \| operator:<br>ssh \| eval test1 = abs ( 40 )<br>ssh \| eval test1 = sin ( Bytes In ) |
| eval <expression> name | n/a | \| eval URL_Length = length ( Request URL ) |
| rename | n/a | \| rename source address as src |
| where | n/a | \| where Bytes In >= 3000<br>\| 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 29
- "Cryptographic Function" on page 29
- "Informational Function" on page 30
- "Mathematical Functions" on page 30
- "Statistical Functions" on page 31
- "Text Functions" on page 32
- "Trigonometry Functions" on page 33

## Comparison and Conditional Functions

| Function | Description | Example |
|---|---|---|
| coalesce(*X*[, *Y*, *Z*,*N*, ...]) | 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.<br>In the list of expressions all elements must be of same type.<br>The only supported types are numeric and string. *X* can be a number, field or expression. | ... \| eval newField = coalesce(null, null,2,3)<br>*Returns*: 2 |
| nullif(*X*,Y) | 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.<br>*X* and *Y* can be a number, field or expression. *Y* must have same data type that *X*. | ... \| eval newField = nullif(2, 3)<br>*Returns*: 2<br>... \| eval newField = nullif(2, 2)<br>*Returns*: null |

## Cryptographic Function

| Function | Description | Example |
|---|---|---|
| md5(*X*) | Calculates the MD5 hash of string, returning the result as a VARCHAR string in hexadecimal.<br>*X* must be a string. | ... \| eval newField = md5('123')<br>*Returns*: 202cb962ac59075b964b07152d234b70 |

## Informational Function

| Function | Description | Example |
|---|---|---|
| isnull(*X*) | Returns true if the *X* is null otherwise returns false. | ... \| eval newField = isnull(2)<br>*Returns*: false |

## Mathematical Functions

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

| Function | Description | Example |
|---|---|---|
| round(*X*, *Y*) | Rounds *X* to the nearest integer. *Y* is the precision to use, if omitted the default precision is zero.<br>*X* can be a number, field or expression. *Y* is a numeric value to indicate the precision. | ... \| eval n=round(1.4)<br>*Returns*: 1<br>... \| eval n=round(1.5)<br>*Returns*: 2 |
| sign(*X*) | Returns a value of -1, 0, or 1 representing the arithmetic sign of the argument. | ... \| eval newField = sign(-8.4)<br>*Returns*: -1<br>... \| eval newField = sign(4)<br>*Returns*: 1<br>... \| eval newField = sign(0)<br>*Returns*: 0 |
| sqrt(*X*) | Takes one numeric argument, *X*, and returns its square root.<br>*X* can be a number, field or expression. | ... \| eval n=sqrt(9)<br>*Returns*: 3 |
| trunc(*X*,*Y*) | Returns the expression value truncated (toward zero).<br>*X* can be a number, field or expression. *Y* is a numeric value to indicate the precision. | ... \| eval newField = trunc(1.9)<br>*Returns*: 1<br>... \| eval newField = trunc(2.89999, 2)<br>*Returns*: 2.89 |

## 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.<br>In the list of expressions all elements must be of same type.<br>The only supported types are numeric and string. *X* can be a number, field or expression. | ... \| eval newField = greatest(7, 5, 9)<br>*Returns*: 9<br>... \| eval newField = greatest('sit', 'site', 'sight')<br>*Returns*: site<br>... \| eval newField = greatest(bytesIn, 100)<br>*Returns*: 100, when bytesIn is less than 100 |

| Function | Description | Example |
|---|---|---|
| least(*X*,*Y*[,*Z*,*N*, ...]) | Returns the smallest value in a list of expressions. The list is up to 20 elements long.<br>In the list of expressions all elements must be of same type.<br>The only supported types are numeric and string. *X* can be a number, field or expression. | ... \| eval newField = least(7, 5, 9)<br>*Returns*: 5<br>... \| eval newField = least('sit', 'site', 'sight')<br>*Returns*: sight<br>... \| eval newField = least(bytesIn, 100)<br>*Returns*: 100, when bytesIn is greater than 100 |
| randomint(*X*) | Returns a random number between 0 and *X*-1.<br>*X* can be any positive integer between the values 1 and 9,223,372,036,854,775,807. | ... \| eval newField = randomint(10)<br>*Returns*: a random number between 0 and 9 |

## Text Functions

| Function | Description | Example |
|---|---|---|
| length(*X*) | Returns the character length of a string, *X*. | ... \| eval n=length(field)<br>*Returns*: the length of (field). If the field is 256 characters long, it returns n=256.<br>... \| eval n=length(“abc”)<br>*Returns*: n=3 (abc is a literal string, surrounded by double quotes) |
| lower(*X*) | Takes a string argument, *X*, and returns the lowercase version. | ... \| eval name=lower("USERNAME" )<br>... \| eval name=tolower("USERNAME" )<br>*Returns*: the value of the field username in lowercase. If the username field contains FRED BROWN, it returns name=fredbrown. |

| Function | Description | Example |
|---|---|---|
| substr(*X*,*Y*,*Z*) | This function returns a new string that is a substring of string *X*.<br>The substring begins with the character at index *Y* and extends up to the character at index *Z*-1.<br>The index is a number that indicates the location of the characters in string *X*, from left to right, starting with zero.<br>*Y* can be negative.<br>*Z* cannot be negative. | ...\| eval n=substr("ArcSight", 5, 6)<br>*Returns*: “g”<br>...\| eval n=substr("ArcSight", 2, 6)<br>*Returns*: “cSig”<br>...\| eval n=substr("ArcSight", 0, 3)<br>*Returns*: “Arc” |
| trim(*X*)<br>ltrim(*X*)<br>rtrim(*X*) | trim(*X*) removes all spaces from both sides of the string *X*.<br>ltrim(*X*) removes all spaces from the left side of the string *X*.<br>rtrim(*X*) removes all spaces from the right side of the string *X*. | For the sake of these examples, assume that *X* is a literal string and _ represents any number of space characters.<br>... \| eval trimmed=ltrim(“_string_”)<br>*Returns*: trimmed=“string_”<br>... \| eval trimmed=rtrim(“_string_”)<br>*Returns*: trimmed=“_string”<br>... \| eval trimmed=trim(“_string_”)<br>*Returns*: “string” |
| upper(*X*) | Takes one string argument and returns the uppercase version. | ... \| eval name=upper(“username”)<br>... \| eval name=toupper(“username”)<br>*Returns*: the value of the field username in uppercase. If username contains fred brown, it returns name=FRED BROWN. |

## Trigonometry Functions

| Function | Description | Example |
|---|---|---|
| | | |
| acos(*X*) | Takes one numeric argument, *X*, and returns its trigonometric inverse cosine. | ...\| eval newField = acos(0.3)<br>*Returns*: 1.2661036727795 |

| **Function** | **Description** | **Example** |
|---|---|---|
| asin(*X*) | Takes one numeric argument, *X*, and returns its trigonometric inverse sine. | ...\| eval newField = asin(3)<br>*Returns*: 0.304692654015398 |
| atan(*X*) | Takes one numeric argument, *X*, and returns its trigonometric inverse tangent. | ...\| eval newField = atan(3)<br>*Returns*: 0.291456794477867 |
| atan2(*X*,*Y*) | Returns a value representing the trigonometric inverse tangent of the arithmetic dividend of the arguments. | ...\| eval newField = atan2(2,1)<br>*Returns*: 1.10714871 |
| cos(*X*) | Takes one numeric argument, *X*, and returns its trigonometric cosine. | ...\| eval newField = cos(3)<br>*Returns*: 2435538 |
| cosh(*X*) | Takes one numeric argument, *X*, and returns its hyperbolic cosine. | ...\| eval newField = cosh(3)<br>*Returns*: 10.0676619957778 |
| cot(*X*) | Takes one numeric argument, *X*, and returns its trigonometric cotangent. | ...\| eval newField = cot(3)<br>*Returns*: -7.01525255143453 |
| ln(*X*) | Takes a number, *X*, and returns its natural log.<br>*X* can be a number, field or expression. | ... \| eval lnBytes=ln(bytesIn)<br>*Returns*: 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.<br>*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)<br>*Returns*: 0.301<br>... \| eval test1 = log (2)<br>*Returns*: 0.301 as it takes the default base as 10 |
| log10(*X*) | (Evaluates the log of number *X* with base 10.<br>*X* can be a number, field or expression. | ... \| eval num=log10(10000)<br>*Returns*: 4 |
| sin(*X*) | Takes one numeric argument, *X*, and returns its trigonometric sine. | ...\| eval newField = sin(3)<br>*Returns*: 0.141120008059867 |
| sinh(*X*) | Takes one numeric argument, *X*, and returns its hyperbolic sine. | ...\| eval newField = sinh(3)<br>*Returns*: 10.0178749274099 |
| tan(*X*) | Takes one numeric argument, *X*, and returns its trigonometric tangent. | ...\| eval newField = tan(3)<br>*Returns*: -0.142546543074278 |
| tanh(*X*) | Takes one numeric argument, *X*, and returns its hyperbolic tangent. | ...\| eval newField = tanh(3)<br>*Returns*: 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 |
| 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<br>agent ip |
| agentHostName | ahost |
| agentId | aid |
| agentMacAddress | amac<br>agent mac |
| agentReceiptTime | art |

| Field | Aliases |
|---|---|
| agentTimeZone | atz |
| agentTranslatedAddress | agent translated ip |
| agentType | at |
| agentVersion | av |
| applicatonProtocol | app<br>protocol |
| baseEventCount | cnt |
| bytesIn | in |
| bytesOut | out |
| categoryBehavior | behavior |
| categoryDeviceGroup | device group |
| categoryObject | object |
| categorySignificance | significance |
| categoryTechnique | technique |
| destinationAddress | dst<br>destination ip<br>destinationip<br>dst ip<br>dest ip<br>target ip<br>targetip<br>target |
| destinationHostName | dhost<br>destination name |
| destinationMacAddress | dmac<br>destination mac |
| destinationNtDomain | dntdom |
| destinationPort | dpt<br>destination port<br>dstport<br>dest port<br>targetport<br>target port |
| destinationProcessId | dpid |
| destinationProcessName | dproc |
| destinationTranslatedAddress | destination translated ip |

| Field | Aliases |
|---|---|
| destinationuserId | duid |
| destinationUserName | duser<br>dst user<br>dest user<br>destination user<br>dst usr |
| destinationUserPrivileges | dpriv |
| deviceAction | act |
| deviceAddress | dvc<br>deviceaddr<br>deviceip<br>device ip |
| deviceCustomFloatingPoint*n* | cfp*n* |
| Valid values for *n* are integers between 1 and 4<br>For example: deviceCustomFloatingPoint1 | For example: cfp1 |
| deviceCustomFloatingPoint*n*Label | cfp*n*Label |
| Valid values for *n* are integers between 1 and 4<br>For example: deviceCustomFloatingPoint1Label | For example: cfp1Label |
| deviceCustomIPv6Address*n* | c6a*n*<br>device custom ipv6 *n* |
| Valid values for *n* are integers between 1 and 4<br>For example: deviceCustomIPv6Address2 | For example: c6a2 |
| deviceCustomIPv6Address*n*Label | c6a*n*Label |
| Valid values for *n* are integers between 1 and 4<br>For example: deviceCustomIPv6Address2Label | For example: c6a2Label |
| deviceCustomNumber*n* | cn*n* |
| Valid values for *n* are integers between 1 and 3<br>For example, deviceCustomNumber3 | For example: cn3 |
| deviceCustomNumber*n*Label | cn*n*Label |
| Valid values for *n* are integers between 1 and 6<br>For example: deviceCustomNumber6Label | For example: cn6Label |
| deviceCustomString*n* | Cs*n* |
| Valid values for *n* are integers between 1 and 6<br>For example: deviceCustomString5 | For example: Cs5 |
| deviceEventCategory | cat |
| deviceHostName | dvchost |

| Field | Aliases |
|---|---|
| deviceMacAddress | dvcmac<br>device mac |
| deviceProcessId | dvcpid |
| deviceReceiptTime | rt |
| deviceTimeZone | dtz |
| deviceTranslatedAddress | device translated ip |
| endTime | end |
| eventOutcome | outcome |
| fileNme | fname |
| fileSize | fsize |
| message | msg |
| requestUrl | request<br>URL |
| sourceAddress | src<br>source ip<br>sourceip<br>src ip |
| sourceHostName | shost |
| sourceMacAddress | smac<br>source mac |
| sourceNtDomain | sntdomain |
| sourcePort | spt<br>srcport<br>src port |
| sourceProcessId | spid |
| sourceProcessName | sproc |
| sourceTranslatedAddress | source translated ip |
| sourceUserId | suid |
| sourceuserName | suser<br>src user<br>source user<br>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 39
- “Enter an IP or MAC Address” on page 39

## How Search Stores IP and MAC Addresses

Search stores IPv4, IPv6, and MAC adresses 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.*`<br>`a.b.*`<br>`a.b.c.*`<br>`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` |
| | Canonical form without consecutive sections of zeroes | `2001:db8::ff00:42:8329` |
| IPv6 in a subnet | Include CIDR notation | `2001:0db8:0000:0000:0000:ff00:0042:8329`<br>`2001:0db8:0000:0000:0000:ff00:0042:8329/24`<br>`2001:db8::/32`<br>**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<br>a-b-c-d-e-f | 94:18:82:6D:63:74<br>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 41
- "Create a Lookup List" on page 41

- "Replace a Lookup List" on page 42
- "Delete a Lookup List" on page 42

## 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 that you want to replace.

3 Select **Replace**.

4 Select the CSV file that 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 that you want to delete.

3 Select the **Trash can** icon.

# Use Specific Sets of Fields for Search Results

You can specify a **fieldset** that determines a group of search result fields to be displayed in the Events table. In the table, each field in the set can provide the 10 most and least common values. Multiple searches can share a fieldset. Search provides a default fieldset that contains the most common event fields. You can customize the default fieldset for individual searches, and you can add lookup list fields to a fieldset.

- "Create a Fieldset" on page 43
- "Modify a Fieldset" on page 43
- "Specify a Default Fieldset" on page 44
- "Delete a Fieldset" on page 44

## Create a Fieldset

1 Select **Search**.

2 Select the name of the current fieldset (shown to the left of the time range selector).

By default, Search displays the name of the last used fieldset.

3 In the **Fieldset Lists** window, select **Create New**.

4 Select and/or deselect the desired fields.

5 To view the complete list of available fields, click **View all**.

6 To locate a specific field, use the search field.

7 To add fields from a lookup list, complete the following steps:

7a Select **Lookup Lists**.

7b Under the name of the desired lookup list, select the fields that you want to include.

8 Specify a name for the new fieldset.

9 Select **Save**.

## Modify a Fieldset

1 Select **Search**.

2 Select the name of the current fieldset (shown to the left of the time range selector).

By default, Search displays the name of the last used fieldset.

3 If the last used fieldset is not the fieldset that you want to edit, select another fieldset from the drop-down menu.

4 Select **Edit**.

5 Select and/or deselect the desired fields.

When you remove a field from a fieldset, Search removes all filters and charts that use that field.

6 Change the name of the fieldset as needed.

7 Add lookup list fields as needed.

8 Select **Save**.

## Specify a Default Fieldset

*You must have Administrator permissions to perform this action.*

You can create a default fieldset to provide a limited number of returned fields and thus improve the search response and performance. Minimizing the number of fields in the default fieldset will not compromise the required fields. When creating a default fieldset, review the following considerations:

- Select a new fieldset other than the default *Base Event Fields* provided with the Search feature.
- Only one fieldset can be designated as the default fieldset. There must be a default fieldset.
- Saved fieldsets are the only ones that can be set as default.
- Each fieldset should have a unique name.
- Fieldset names are not case sensitive.
- A default fieldset cannot be edited and saved under the original name.

## Delete a Fieldset

You can delete a fieldset that you have created or that has not been designated as a default fieldset. If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search.

1. Select **Search**.
2. Select the name of the current fieldset (shown to the left of the time range selector).

   By default, Search displays the name of the last used fieldset.
3. If the last used fieldset is not the fieldset that you want to delete, select another fieldset from the drop-down menu.
4. Select **Edit this set**.
5. Select **Delete**.

# 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 reexecuting 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 45
- "Base the Search on the Timestamp for Events" on page 45
- "Understand How Time Zones Affect Search Results" on page 46

## 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 |
| $CurrentWeek | Midnight of the previous Monday (or same as `$Today` 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 than 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 29 May 1975 when the current date in the database when the database received the event is 29 June 2020. The database recognizes that the event's 29 May 1975 timestamp for DRT is outside the credible time range. Based on the discrepancy with DRT, the database sets NET to 29 June 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.

# II 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 display those dashboards by default.

# 4 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 display specific dashboards by default.

- "View a Dashboard" on page 49
- "View a Report" on page 50
- "Choose Default Dashboards for the Reports Portal" on page 50

## 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

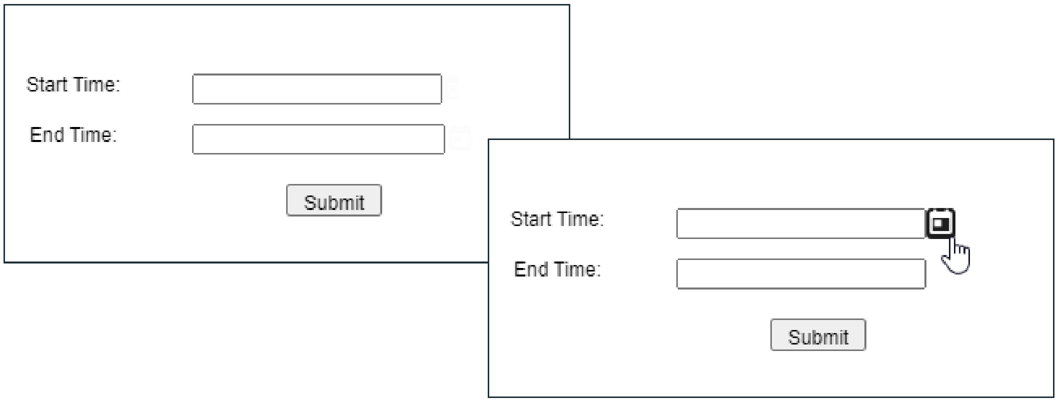
When you open a report, you must define the time range for the data you want to view.

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 **(?)**.

# 5 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 ID**s) on the MITRE ATT&CK website (https://attack.mitre.org/).

| Dashboards | Reports |
|---|---|
| MITRE ATT&CK Overview<br>Evaluation Techniques and Tactics Summary | MITRE ATT&CK Destination Address Summary<br>MITRE ATT&CK Destination Host Summary<br>MITRE ATT&CK Destination Username Summary<br>MITRE ATT&CK Source Address Summary<br>MITRE ATT&CK Source Hostname Summary<br>MITRE ATT&CK Source Username Summary<br>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 54
- "Evaluation Techniques and Tactics Summary" on page 54

## 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 indicted 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 55
- “MITRE ATT&CK Destination Host Summary” on page 55
- “MITRE ATT&CK Destination Username Summary” on page 56
- “MITRE ATT&CK Source Address Summary” on page 56
- “MITRE ATT&CK Source Hostname Summary” on page 56
- “MITRE ATT&CK Source Username Summary” on page 56
- “MITRE ATT&CK Technique Summary” on page 57

## 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 infomration 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

# 6 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). 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<br>EC2 Instances Communicating with Cryptcurrency Entity<br>EC2 Instances Querying Domains Involved in Phishing Attacks<br>EC2 Machines Involved in Suspicious Communication<br>Email Spam Originated from EC2 Instances<br>Nefarious Activity by an Unauthorized Individual from EC2<br>Suspicious Activity Reported by Microsoft Azure<br>Trojans or Backdoors Installed on EC2 Instances | *n/a* |
| Account Hijacking | Account Hijacking Vulnerabilities<br>Man in the Middle Attacks<br>Phishing Attacks<br>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 | *n/a* |
| Data Breaches | All Information Leakage Events<br>Information Disclosure Vulnerabilities<br>Organizational Information Leakage<br>Personal Information Leakage | *n/a* |

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

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

| Category | Dashboards | Reports |
|---|---|---|
| Vulnerability Monitoring | *n/a* | High Risk Vulnerabilities by Host<br>SSL Vulnerabilities<br>Vulnerability Summary by Host<br>XSRF Vulnerabilities<br>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 addreses 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 enteprise. 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 Atacks

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 detinations 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 proactively 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 vulnerabilties, 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.

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

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 vulernabilities 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 shwoing 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 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.

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

**Misconfiguration Events Overview**

Provides an overview of the misconfigured events reported in your environment. The charts show the top misconfigured systems, the top misconfiruation 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 antivirus 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 misconfigured XML processors use XML documents to evaluate external entity references, and can inadvertently process harmful XML input. Malicious users 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.

# III 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.

# 9 Generating Models to View Anamalous Data

*You must have Administrative 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

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**.

# 10 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

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 exfiltration 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 overtime.

# 11 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 timeframe. This category uses the following formula:

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

# 12 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.

# 13 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.

**Data Timeseries**

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.

# V 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 14, “Accessing Reports and Dashboards,” on page 101
- Chapter 15, “Scheduling Report Generation,” on page 103
- Chapter 16, “Designing Reports for Data Analysis,” on page 105
- Chapter 17, “Adding and Removing Report Content,” on page 107

# 14 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.

# 15 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.

# 16 Designing Reports for Data Analysis

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

Select **Reports** > **Designer**.

Report **Designer** provides a wizard that allows you to create new reports and dashboards 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.

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.

# 17 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, and MS Access. Be sure to download the latest driver (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.

# VI 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.

# 18 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

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

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*. You change a storage group’s status to inactive to prevent new events from being sent to the group. 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 113
- "Apply Your Changes to a Storage Group" on page 113

## 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 114

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.

# VII 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.

# 19 Assigning Permissions for Recon

To view your permissions, select **your_ID** > ***My Profile*** > **Permissions**.

- "Default Permissions for Searches" on page 117
- "Default Permissions for Reports" on page 117
- "Additional Permissions for Administrators" on page 118

## Default Permissions for Searches

The Search feature provides the following default permissions:

| Permission | Allows users to... |
|---|---|
| Execute Search | Execute searches using fieldsets, custom ranges dates, and search operators |
| Export Search Results | Export the search results in csv format |
| Manage Outlier Models and Scoring | Create and delete Outliers models<br>Build and pause the scoring processes |
| Manage Lookup Lists | Add, configure, view, and delete lookup lists |

## Default Permissions for Reports

The Reports feature provides the following permissions:

| Permission | Allows users to... |
|---|---|
| Report Admin | ◆ View dashboards and reports<br>◆ Create subfolders<br>◆ Account logout<br>◆ Schedule reports<br>◆ Create data worksheets, dashboards, and reports<br>◆ View Admin reports<br>◆ Manage the data source |
| Design Reports | ◆ View dashboards and reports<br>◆ Create subfolders<br>◆ Account logout<br>◆ Schedule reports<br>◆ Create data worksheets, dashboards, and reports |

| Permission | Allows users to... |
|---|---|
| Schedule Reports | - View dashboards and reports<br>- Create subfolders<br>- Account logout<br>- Schedule reports |
| View Reports | - View dashboards and reports<br>- Create subfolders<br>- Account logout |

## Additional Permissions for Administrators

In addition to the administrative permissions available with the Fusion capability, an administrator can have the following permissions:

| Permission | Allows users to... |
|---|---|
| Access Database Monitoring | Access to the database monitoring APIs |
| Manage Storage Groups | Create and manage storage groups |

# 20 Default Roles for Recon

Select **ADMIN**> **Roles**.

When you deploy Recon, the default roles provided for the common services in Fusion adapt to include appropriate Recon permissions. The common services include the Dashboard.

| Default Role | Permissions |
|---|---|
| System Admin | ◆ All **Admin** and both **Dashboard** permissions<br>◆ All **Recon** permissions |
| Admin | ◆ All **Admin** and both **Dashboard** permissions<br>◆ All **Recon** permissions |
| Analyst L1 | ◆ Both **Dashboard** permissions<br>◆ Execute Search permission |
| Guest | ◆ Both **Dashboard** permissions<br>◆ Execute Search permission |
| Report User | Report **Admin** permission |
| User | ◆ Both **Dashboard** permissions<br>◆ Execute Search permission |

You can create new roles that reflect your organization's needs. You cannot change the permissions of the System Admin role.

# 21 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 121

## 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 that you regularly use for a search. The default value is *Base Event Fields*.

**Default View**

Specifies whether you want the Events Table to display 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.

- Browser
- Database
- Custom

To specify the type of timestamp that you want to use, modify the preference for **Base Searches On**.

**Date / Time Format**

Specifies the format of dates and times that you want Search to use. The default is `YYYY/MM/DD`.

For example, you might want to use the same format that you have already configured for your browser. Alternatively, you might prefer a format like `MM/DD/YYYY HH:MM:SS`.

### Default Time Setting

Specifies the time range within which you want Search to find events. The default is *Last 30 minutes*.

- **Dynamic**

  If you prefer to use a dynamic time range, you must also specify the **Start** and **End** times. For example, specify *$Now - 30m* and *$Now* respectively.

- **Static**

  If you use different time settings for each search that you create, you might want to select this option for your preference. The default is the preset value of *Last 30 minutes*.

- **Preset**

  If you prefer to use a preset time range, you must also specify a preset value. For example, *Last 24 hours*.

### Base Searches On

Specifies the timestamp associated with the events that you want to find:

- Normalized Event Time
- Device Receipt Time
- Database Receipt Time

### Search Expires In

Specifies how often you want searches to expire, and thus be removed from the system. This option enables you to reduce the amount of search results held in the database, and thus enabling Search performance. The database purges expired searches at midnight. The default is 30 days, with a maximum of 365 days.

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-rujning the search, as well as saving the search.

### Maximum Search Results

Specifies the maximum number of events that the Search will return. You can specify a value between 1 and 10 million. The default is *3,000,000*, unless otherwise specified in the CDF Management Portal. This option cannot override the limit specified in the Management Portal.

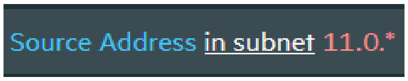
Search considers a search complete when the results reach the maximum limit.

### Highlight Query Syntax

Specifies whether you want Search to use color to differentiate the syntax terms from the operators and functions within the query.

For example, in the figure below, Search displays the variable *Source Address* in blue, the value *11.0.** in red, and the operator *in subnet* in white.

***Figure 21-1*** *Example of Highlighted Query Syntax*



Source Address in subnet 11.0.*