OpenText
ArcSight Platform

Software Version:

User's Guide for ArcSight Platform 23.3 and ArcSight SIEM as a Service 23.9.1

Document Release Date:

Software Release Date:

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number

- Document Release Date, which changes each time the document is updated

- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

Welcome to ArcSight

This *User's Guide* for ArcSight Platform and ArcSight SIEM as a Service provides concepts, use cases, and contextual help with the following activity:

- Create and use ArcSight dashboards to analyze data

- Search for events

- Check the integrity of your data

- Analyze aggregated data with outlier analytics

- Access the Reports Portal to create visuals and reports for analyzing data

- Hunt for known threats and vulnerabilities with built-in reports

- Respond to alerts and manage cases

- Manage your MSSP profile and submit monthly EPS usage reports

- Access ArcMC to manage and monitor components in the ArcSight infrastructure

- Manage users and groups of users

- Manage your user profile

- Check whether your environment complies with standards for handling sensitive data

- Manage ingested and imported data

About this Guide

This User's Guide provides concepts, use cases, and contextual help for many of the features in ArcSight Platform and ArcSight SIEM as a Service, including the common layer of services. For the most recent version of this guide, see links to the documentation sites in Additional Documentation below.

Intended Audience

This book provides information for individuals who need to search events and check for vulnerabilities; respond and manage incidents; create users, groups, and roles; create and run reports and dashboards, and use the ArcSight Dashboard. These individuals have experience using security and identity management products, as well as creating reports and dashboards. Some users might need experience in managing service provider contracts.

Additional Documentation

This documentation library includes the following resources, based on the product that you use:

ArcSight SIEM as a Service (SaaS)

- *ArcSight SIEM as a Service - Quick Start Guide for Administrators*, which provides an overview of the products deployed in this suite and their latest features or updates

- User Guides and Release Notes for the capabilities that deployed in your ArcSight SaaS environment

- Documentation site for ArcSight SIEM as a Service

ArcSight Platform (for installing on-premises, AWS, and Azure)

- *Release Notes for ArcSight Platform 23.3*, which provides information about the latest release

- *Administrator's Guide to ArcSight Platform 23.3*, which provides concepts, use cases, and guidance for installing, upgrade, managing, and maintaining the ArcSight Platform in your environment

- *Technical Requirements for ArcSight Platform 23.3*, which provides information about the hardware and software requirements for installing ArcSight Platform and the deployed capabilities in your environment

- *ArcSight Platform Upgrade Paths*, which provides information about the paths to upgrade to the latest release from your current release

- *ArcSight Solutions and Compliance Insight Packages*, which provide a complete set of compliance and audit related packages and documentation

- Documentation site for ArcSight Platform where you can discover documentation for multiple ArcSight products

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 Open Text Customer Care.

Creating and Using ArcSight Dashboards

Available only with ArcSight capabilities.

Select **Dashboard**.

The **Dashboard** enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be deployed in your security environment:

- Managing and monitoring ArcSight infrastructure components with ArcSight Management Center (ArcMC)

- Real-time event monitoring and correlation with data from ArcSight Enterprise Security Manager (ESM)

- Analyzing end-user behavior with ArcSight Intelligence

- Performing deep-dive investigations with Log Management and Compliance (Recon)

- Responding to and mitigating cyber attacks with ArcSight SOAR

To help you get started, the system provides a set of out-of-the-box widgets and dashboards. Users can organize the widgets into personalized dashboards. Out-of-the-box, any user can perform the following actions:

- View dashboards owned by or shared with the user

- Modify, delete, and export dashboards owned by the user

- Create or clone dashboards

- Import dashboards

- Set a dashboard as a personal default dashboard

You can create one or more ArcSight dashboards that incorporate widgets in your preferred arrangement. Depending on your role, you can create dashboards to be shared with specific roles, and even identify which of those dashboards should be the default landing page for a role.

Viewing a Dashboard

Select **Dashboard**.

The Dashboard automatically displays your default dashboard when you log in or select **Dashboard**. If you do not have a default dashboard, the Dashboard displays the list of available dashboards.

While viewing a dashboard, you can modify its settings or clone it to create a new dashboard.

View Data in a Dashboard

Select **Dashboard**.

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

View a Different Dashboard

When viewing a dashboard, select **View All Dashboards**.

In the course of your day, you might need to switch among several dashboards. You can view the list of dashboards in two ways:

- Favorite Dashboards
- All Available Dashboards

The list indicates whether a dashboard is shared, for your personal use, or assigned as the default for a role. You can also see who owns each dashboard. An "out-of-the-box" label indicates that the dashboard is provided with the Dashboard. In general, out-of-the-box dashboards are available only to the Dashboard administrator because they require configuration before use.

Favorite Dashboards

You can specify which dashboards are your favorites.

All Available Dashboards

You can view the full list of available dashboards. A star beside the name indicates that you have marked that dashboard as a favorite.

Viewing Analyst and Entity Details

Some of the widgets in the dashboard allow you to review activity associated with specific cases, case owners or owner groups, and entities.

Case Overview by Owner

Select an owner in a widget.

You can review all cases currently assigned to a specific owner. When you select an owner in a widget, the Dashboard opens the **Case Overview by Owner** page. For each case, the table includes the following details:

- Severity of the case

- Current stage of the case

- Length of time that the case has been assigned to the owner

- Time since the case was created

- Time since the case was last updated

To determine when the owner received a particular case, hover over the **Owned** field. If you hover over the **Created** and **Last Updated** fields, the Dashboard shows the specific date and time that the case was created or last updated, respectively.

Review Entities

Requires ArcSight Intelligence be deployed. This feature is not available in the ArcSight SaaS environment.

Select an entity in a widget.

You can explore the entities and their risky behaviors in the following ways:

- When you select an entity type in the Entity Count Overview widget, the Entities page opens in the ArcSight Intelligence UI, where you can view the details of the risky entities of the selected entity type. You can also navigate to the Entities page in the ArcSight Intelligence UI in the following ways:

  ◦ When you have deployed only ArcSight Intelligence, click **ENTITIES AT RISK** in the left pane.

- ○ (Non-SaaS only) When you have deployed ArcSight Intelligence and Recon, click **INSIGHTS** > **Entities At Risk** in the left pane.
- When you select an entity in the Top Risky Entities widget, the Explore page opens in the ArcSight Intelligence UI, where you can explore the risky activities associated with the entity.

Managing Dashboards and Content

Select **Dashboard**.

You can add, remove, and rearrange the order of widgets in a dashboard. You can also change the content of a widget then save it with a unique name. To edit a dashboard, you must be currently viewing it.

Understand the Provided Dashboards

To help you get started, the Dashboard provides out-of-the-box dashboards with associated widgets. You will need to configure the widgets to ensure the dashboards display data appropriately for your environment.

- Data Processing Monitoring

- Health and Performance Monitoring

- How is My SOC Running?

- Entity Priority

- Entity Risk

Initially, the out-of-the-box dashboards are available to the administrative user created during the initial log in. This user can share these dashboards with SOC team members, who can then create their own clones for custom dashboards. Alternatively, administrators can create one or more clones based on these dashboards, then share the clones, and set default dashboards for roles.

Data Processing Monitoring

Requires that at least one deployed capability uses the ArcSight Database.

The dashboard, **Data Processing Monitoring**, provides information to monitor the rate of event ingestion into the ArcSight Database. It includes the following widget:

- Database Event Ingestion Timeline

Health and Performance Monitoring

Requires that at least one deployed capability uses the ArcSight Database.

The dashboard, **Health and Performance Monitoring**, provides information about the status of the ArcSight Database. It includes the following widgets:

- Database Cluster Node Status
- Database Event Ingestion Timeline
- Database Storage Utilization

How is My SOC Running?

Requires ArcSight ESM Command Center be deployed. This dashboard is not available in the ArcSight SaaS environment.

The dashboard, **How is my SOC running?**, gives you an overview of the status and trends related to ESM case management. It includes the following widgets:

- Case Breakdown
- Case Load
- Case Timeline
- Case Workflow Analysis
- Productivity
- Threat Analysis Funnel

Entity Priority

Requires ArcSight Layered Analytics capability be deployed. This dashboard is not available in the ArcSight SaaS environment.

The dashboard, **Entity Priority**, combines content from ArcSight ESM and Intelligence to provide the status of users and entities at risk. It includes the following widgets:

- Active List
- Entity Count Overview

Entity Risk

Requires ArcSight Intelligence be deployed. This dashboard is not available in the ArcSight SaaS environment.

The dashboard, **Entity Risk** provides at-a-glance actionable information on the current, overall risk of your organization. It includes the following widgets:

- Analytics Pipeline
- Entity Count Overview

- Overall Risk Level
- Top Risky Entities

The dashboard provides the following information:

- Risk statistics: number of events analyzed, number of anomalies and violations found, and the number of active risky entities.

- The types of entities involved and their risk counts. When you click an entity type, the Entities page opens in the ArcSight Intelligence UI, where additional information for the selected entity type is displayed.

- The trending risk of the organization.

- The dominant potential threat, if any.

- The top 5 risky users. When you click a user, the Explore page opens in the ArcSight Intelligence UI, with the selected user's name applied to the anomalies and violations filter.

- An option to download a PDF containing a detailed report of the risk of the organization. For more information about PDF report, see the "PDF Reports" section in the *ArcSight Intelligence User's Guide*.

Change the Time Range of Data in a Dashboard

When viewing a dashboard, select ✎.

Most of the widgets in a dashboard display data according to the either a specified **Time range** or an **As of now** setting, which displays data based on the last time that you refreshed the browser. You can configure the time setting.

If you select a preset time, the Dashboard displays data starting from 12:00:00 a.m. of the first date in the range to 11:59:59 p.m. of the last date in the range. If the last date is the current date, then the Dashboard defaults to the current time or time of the last browser refresh. For example, the **Last 1 month** setting might be from 12:00:00 a.m. April 29 to 3:34 p.m. May 29. Note that the Dashboard does not display minutes and hours.

To display time values, the Dashboard uses your browser settings, such as your local time zone.

Create or Clone a Dashboard

You can build as many dashboards that you need either by creating a new dashboard or copying a custom or out-of-the-box dashboard.

- Create a Dashboard
- Clone a Dashboard

Create a Dashboard

You can create as many dashboards as you need.

1. (Conditional) From within an existing dashboard, select ... > **Create new Dashboard**.

2. (Conditional) From the Dashboards list, select **+**.

3. Specify a **Title** for the new Dashboard.

   The title can be a maximum of 150 characters, and must be unique.

4. To add a widget, select **+** beside **Main Context**.

5. Choose the widget that you want to add.

6. Modify the widget's properties.

7. Continue to add widgets as needed.

8. Arrange the widgets how you prefer.

9. **Save** your changes.

   Alternatively, you might choose to clone an existing dashboard or import a dashboard that someone else created.

Clone a Dashboard

To quickly create dashboards, you can copy an existing dashboard. For example, Inez Bates wants to customize an out-of-the-box dashboard and share it with her APJ analyst team. She clones the dashboard, then modifies some of the widgets to include only cases that the team owns.

By default, the Dashboard copies the name of the original version and adds "Copy of" to the name. You can change that title as part of the cloning process or edit the title later.

1. From within an existing dashboard, select ... > **Clone**.

2. Specify a unique name for the new dashboard.

3. (Optional) Indicate that you want to add the new dashboard to your Favorites.

4. **Save** your changes.

   Alternatively, you can import a dashboard that someone else created.

Modify a Dashboard

While viewing a dashboard, select ✏.

You can only change the configuration of the dashboard that you are currently viewing, such as editing a widget's properties or adding and removing widgets.

- Add Widgets
- Modify a Widget's Properties
- Rearrange the Order of Widgets
- Remove Widgets
- Change the Dashboard's Name

Add Widgets

While viewing a dashboard, select 🖉, then + in Main Context.

To find an existing widget, you can search by its name or the tags assigned to it. After choosing the widget, you can change its properties to suit your dashboard.

To group widgets in sections under the **Main Context**, select **Nested Context** from the widget selector or select a context that has already been added to the dashboard. Then you can add widgets in that section. You can also change the name of the sections.

Modify a Widget's Properties

While viewing a dashboard, select 🖉.

To edit the settings of a widget, select the widget. Make your changes in the **Widget Properties** pane. Then save your changes.

Rearrange the Order of Widgets

While viewing a dashboard, select 🖉.

To rearrange the order of widgets in a dashboard, simply drag each widget to the new location. Then save your changes.

Remove Widgets

While viewing a dashboard, select 🖉.

To remove a widget, select X within the widget's boundaries. Then save your changes to the dashboard.

Change the Dashboard's Name

While viewing a dashboard, select 🖉.

The title of a dashboard can be a maximum of 150 characters, and must be unique.

Mark a Dashboard as a Favorite

To more quickly find a dashboard, you can add it to your **Favorites** list.

While viewing a dashboard, select ☆.

Specify a Default Dashboard

Select … > **Set as default for me**.

When you log in, the Dashboard automatically displays the default dashboard that you have chosen or that an Administrator has assigned for your role. If no dashboard has been assigned to you or no default exists, you will see the list of available dashboards.

To override the default dashboard assigned to your role, you can specify any currently displayed dashboard as your preferred landing page.

Share a Dashboard

*You must have the **Share Dashboard** permission to perform this function.*

Select … > **Share**.

You can share the currently displayed dashboard with one or more of your assigned roles. If you have the **Manage Roles** permission, you can share the dashboard with any role.

Alternatively, if you cannot share a dashboard, you can export the dashboard for others to import and use.

> You cannot re-share a dashboard that has been shared with you.

Import and Export a Dashboard

As an alternative to sharing or copying a dashboard, you can export the dashboard as a json file for other users to import to their Dashboard. The json file contains information about the dashboard's configuration and the included widgets. The file does not contain any data displayed in the dashboard. You can modify the exported json file or edit the imported dashboard.

For example, Inez Bates on the APJ analyst team really likes a dashboard that **Murphy Buckley,** on the EMEA team, made for his personal use. Murphy could share this dashboard with Inez. However, the widgets are configured for the AMS team's use, so the data would not be useful for Inez. Instead, Murphy exports the dashboard and sends the json file to

Inez. She imports the dashboard, then modifies some of the widgets to point to cases that she and the APJ team own.

- Considerations for Importing a Dashboard
- Import a Dashboard
- Export a Dashboard

Considerations for Importing a Dashboard

Changing the json file of a dashboard can cause problems either during import or within the Dashboard. Usually, you only need to change the name of the dashboard in the file. Before importing a dashboard, please review the following considerations:

- You cannot import a dashboard whose name already exists in your Dashboard environment. Ensure that you change the title of the dashboard in the json file.

  > This caveat includes names of dashboards that other users have created and which you might not see in your list.

- You cannot import a dashboard if it contains widgets that do not exist in your Dashboard environment.

Import a Dashboard

When viewing the list of Dashboards, select … > **Import Dashboard**. Then browse to the appropriate json file.

Export a Dashboard

When viewing a Dashboard, select … > **Export Dashboard**.

Display a Dashboard on the SOC Screen

Like most software, the Dashboard will end a session that has been idle for a while. This is good for security. However, it can be inconvenient if you display a dashboard on the large monitors in your SOC. To avoid manually interacting with the browser or logging in

regularly, you can use a plug-in that automatically refreshes all content in the browser tab that displays the dashboard.

To automatically refresh dashboards on the SOC screen:

1. Install an Auto Refresh add-on for your browser.

   There are free add-ons available for supported browsers.

2. Specify the time interval after which you want the browser tab to refresh automatically.

   For instance, if you set the time for auto-refresh to five minutes, your browser tab will refresh automatically after an interval of five minutes.

3. (Optional) Minimize the left navigation pane.

Note that, when you refresh the tab, the Dashboard always updates to the latest data based on your chosen time range.

Configuring Widgets

Widgets display data according to your specifications. You can filter content by specific case owners or groups, case severities, and sub-filters.

Understand Widget Properties

When you configure a widget, you might see a combination of some or all of the following properties:

Title and Subtitle
> Specifies the name and an optional secondary name for a widget you want to add to your dashboard.
>
> You can also specify whether the dashboard displays the title or subtitle.
>
> In general, because you might have several variations of some widgets, it's a good practice to title each widget according to your sub-filter criteria. For example, SOC Manager Franz Tupper creates a Case Breakdown widget for each of the SOC's three owner groups: EMEA, AMS, and APJ. He names the widgets *Case Breakdown-EMEA*, *Case Breakdown-AMS*, and *Case Breakdown-APJ*.

Severity
> Specifies the categories of importance, or severity, assigned to the affected cases. For example, in ESM, some cases might be categorized as *Catastrophic* or *Marginal*.
>
> When selected for **Group by** or **Facet**, you can add sub-filters by specifying the type of Cases, Assigned Owners, or Assigned Owner Groups that you also want to view.

Assigned Owners
> Indicates that you want to display data based on the individuals assigned to the affected cases. You can specify the **Owners** that you want to include.
>
> If you do not specify an owner, the Dashboard includes data for all owners. If you specify more than five owners, the Dashboard displays data for the top five selected owners. Then adds an **Other** category that totals the values for all other selected owners.
>
> When selected for **Group by**, you can add sub-filters by specifying the type of Cases and Importance categories that you also want to view.

Assigned Owner Groups
> Indicates that you want to display data based on the owner groups, or teams, assigned to the affected cases. The widget also displays all cases assigned to the individuals and

child groups within the owner groups. You can specify the **Owner Groups** that you want to include.

If you do not specify an owner group, the Dashboard includes data for all groups, and thus all owners. If you specify more than five owner groups, the Dashboard displays data for the top five selected groups. Then adds an **Other** category that totals the values for all other selected owner groups.

When selected for **Group by**, you can add sub-filters by specifying the type of Cases and Severity categories that you also want to view.

Assigned Cases

Applies only when you specify Severity for Group by

Indicates whether a sub-filter includes cases assigned to the specified owners.

To include specific owners or owner groups, select Owners then add the names that you want to include. Otherwise, the Dashboard displays data for all assigned cases.

In general, to view sub-filter data, you might hover over the visual in the widget or drill down into the data.

Unassigned Cases

Applies only when you specify Severity for Group by

Indicates whether a sub-filter includes unassigned cases.

Number of Groups

Applies only to the SOAR Productivity widget

Indicates whether a sub-filter includes the most productive number of groups.

Statuses

Applies only when you specify Statuses for Facet

Indicates whether a sub-filter includes statuses.

Show Top N Playbooks

Applies only to the SOAR Productivity widget

Indicates whether a sub-filter includes the number of Top Playbooks executed.

Classifications

Applies only to the SOAR Productivity widget

Indicates whether a sub-filter includes the classification of the attack type.

Number of Playbooks

Applies only to the SOAR Productivity widget

Indicates whether a sub-filter includes the number of Playbooks executed.

Target for Case Closure

Applies only to the Productivity and Case Load widgets.

Specifies the number of cases per week that you expect each owner group (Productivity widget) or owner (Case Load) to close.

Time Range

Specifies the start and end dates for the data that you want to view:

- **Dashboard's default** tells the widget to use the time range set for the dashboard.

- **As of now** tells the widget to use the most recent data retrieved from the data source.

  Data updates each time you refresh the browser, unless you have specified a **Custom** time range.

  > You can set a **maximum time range** to limit the amount of data that the Dashboard can collect from its data sources. For example, you can specify 365 days of data. For more information, see the *Administrator's Guide to ArcSight Command Center for ESM*.

To assign or change the severity or owner of a case, use the ArcSight Console or Command Center.

Layout

Specifies the orientation of the widget in a custom dashboard. For example, you might want the *Database Event Ingestion Timeline* widget to span the width of the dashboard.

Understand the Provided Widgets

The Dashboard ships with several widgets designed to help you manage your security operations. When you create or modify a dashboard, you can choose from the full set of widgets and configure them as needed.

The Dashboard provides the following out-of-the-box widgets:

- Active List

- Analytics Pipeline

- Case Breakdown

- Case Load

- Case Timeline

- Case Workflow Analysis

- Database Cluster Node Status

- Database Event Ingestion Timeline

- Database Storage Utilization

- Entity Count Overview

- Overall Risk Level

- Productivity

- SOAR Productivity

- SOAR Average KPI for Event

- SOAR Case Breakdown - Severity

- SOAR Case Load

- SOAR Case Status

- SOAR Threat Analysis Funnel

- SOAR Case Timeline

- SOAR Top Playbooks Executed

- SOAR Trend - Playbooks Executed

- SOAR Trend - Mean Time To Resolve

- SOAR Trend - Mean Time To Respond

- Threat Analysis Funnel

- Top Risky Entities

Active List

Requires ArcSight Intelligence and ArcSight ESM be deployed for best effect. This widget is not available in the ArcSight SaaS environment.

To watch for suspicious activity associated with entities, add **Active List** widgets to your dashboard. Each widget displays the top five at-risk entities, based on the specified **Active list**, **Field**, and **Entity type** settings with both ESM and ArcSight Intelligence installed.

The available active lists correspond to active lists in ESM. For example, you might have watch lists for privileged or administrative users or vulnerable hosts. If an active list entry matches an entity in ArcSight Intelligence, then the widget also shows the ArcSight

Intelligence risk score for that entry. However, if the ArcSight Intelligence capability is not deployed, the widget cannot display risk scores but just entities in alphabetical order.

Analytics Pipeline

Requires ArcSight Intelligence be deployed. This widget is not available in the ArcSight SaaS environment.

The **Analytics Pipeline** widget provides the risk statistics for the last analytics run. It displays the number of events analyzed, the number of anomalies and violations found, and the number of active risky entities. This widget also provides the option of downloading a PDF report detailing the current risk of the organization. You can select the orientation of the widget as **Landscape** or **Portrait**. The default orientation is **Landscape**.

Case Breakdown

Requires ArcSight ESM be deployed. This widget is not available in a SaaS environment.

The **Case Breakdown** widget displays the number or percentage of cases by their **Severity**, **Owners**, or **Owner Groups**. The widget always shows data **As of Now**, regardless of the specified time range for the dashboard.

By default, the widget shows data for total open, assigned cases. The widget displays a maximum of six data points, which comprise the top five objects associated with the specified filter plus an *Other* object that combines the rest of the cases. For example, if you have seven case owners, the widget shows specific values for the five owners with the largest quantity of cases, then groups the total number of cases for the other two owners in the Other category.

You can change the widget's properties to view cases in a different state, such as cases created by specific analysts. For example, SOC Manager Franz Tupper wants to view all cases created by his Level 1 analysts. He sets the filter to **Assigned Owners**, and in the sub-filters specifies Jin Stafford, Neve Marshall, Troy Leach, and Chole Gay as **Owners**. Then he selects **Created** for the state that he wants to analyze. The widget will display the quantity and percentage of cases created by each analyst. Because Franz has configured the dashboard to automatically refresh, he sees in real-time when the analysts add new cases.

If you don't specify an owner or owner group, the widget displays data for all cases.

Case Load

Requires ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

To help managers balance the amount of work assigned to case owners, the **Case Load** widget provides several case management metrics:

- Average number of cases each owner closes per week

- Estimation of the time required to close all cases currently assigned to the owner based on the time elapsed since the cases were opened

- Projection of the number of cases per severity that the owner might not be able to close, based on the configured target, the time elapsed since the cases were opened, and the average velocity of the owner. This assumes that owners work on cases in severity order, from highest to lowest.

By default, the widget shows the data for total open, assigned cases for the top three members of the group based on their average number of cases per week. You can filter the data by specific **Owner Groups**. The metrics are based on the specified time range and the target number of cases that you expect the owners to close per **Severity**

For best use of this widget, it is recommended that you create one Case Load widget per owner group. In this way, you will see details for members of the owner group.

Case Timeline

Requires ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

The **Case Timeline** widget shows changes in the volume of cases over a specified time range. By default, the widget filters the data according to the **Severity** category assigned in ESM. However, you can also choose to view trends for other case states, such as cases **Closed** by specific **Owners** or **Owner Groups**.

To observe the breakdown of cases associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

Case Workflow Analysis

Requires ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

The **Case Workflow Analysis** widget helps you compare the current volume of cases per stage with how the cases transitioned among the stages. In the widget, the width of the lines indicates the average time cases have taken to move from stage to stage during the specified time range. The diameter of each circle, except for the *Closed* stage, represents the total number of cases currently at that stage, based on the last refresh of data from the source.

> The widget does not represent backward transitions. For example, a case moves from *Final* back to *Follow-up* during the specified time range.

By default, the widget shows data for total open, assigned cases. You can also choose to filter the data by **Severity**, **Owners**, or **Owner Groups**.

Database Cluster Node Status

Requires that at least one deployed capability uses the ArcSight Database.

The **Database Cluster Node Status** widget helps SOC managers and IT administrators monitor the state of the nodes that host the database. This widget displays the state of each node in the database cluster. It also raises awareness that the number of nodes that are down can affect the resiliency of the database cluster. For example, if the database resiliency setting is 1, and two of three nodes go down, then the database might automatically shut down to protect itself.

Also, when nodes are down or recovering from a failure, it's possible that you might experience data loss. The longer that a node is offline, the longer it will take to recover because it needs to acquire the data available in the rest of the cluster.

Database Event Ingestion Timeline

Requires that at least one deployed capability uses the ArcSight Database.

To help SOC managers and IT administrators monitor the rate of event ingestion into the database, use the **Database Event Ingestion Timeline** widget. Due to differences in how quickly an event from different sources arrives at the database for storage, the moment when a database stores an event differs from when the event occurred. This widget measures when the database receives the event data.

Database Storage Utilization

Requires that at least one deployed capability uses the ArcSight Database.

To help SOC Managers and IT Administrators ensure that disk use does not overload the database nodes, the **Database Storage Utilization** widget displays storage utilization data for up to five database nodes. In general, most administrators keep disk usage below 60 percent per node, thus ensuring space for temporary activity required by some query execution operators.

If the database cluster has more than five nodes in the cluster, you might specify the nodes with the least amount of free space available. In this way, you can monitor the nodes at most risk of running out space. For each node, you can compare the percent and quantity of

space used to the total amount. You can also monitor the throughput and latency of the database per second.

The ArcSight Database supports use of a third party storage location technology, shared among its database nodes on premises or cloud. This shared storage location is also called Communal Storage and represented in the associated widget.

> The computational and communal layers of the database are separate and allows storage of data in a single location with the ability to elastically vary the connected computer nodes per necessary computational needs. For more information, see the *Administrator's Guide to ArcSight Platform*.

Entity Count Overview

Requires ArcSight Intelligence be deployed. This widget is not available in the ArcSight SaaS environment.

To help identify users and entities currently at risk in your organization, the **Entity Count Overview** widget displays the number of entities involved in risky behaviors, by entity type, along with their risk counts based on the last analytics run. When you click an entity type in the widget, the Entities page opens in the ArcSight Intelligence UI, where additional information for the selected entity type is displayed.

Overall Risk Level

Requires ArcSight Intelligence be deployed. This widget is not available in the ArcSight SaaS environment.

To help understand the general risk in your organization, the **Overall Risk Level** widget displays the trending risk of the organization based on the last analytics run.

Productivity

Requires ArcSight ESM be deployed. This widget is not available in a SaaS environment.

To help managers optimize analyst activity for the specified time range, the **Productivity** widget incorporates several elements related to SOC productivity:

Case Closure Velocity
Shows the current rate of case closure per week based on the target velocity for all owners and owner groups. For example, you might expect teams to close at least 5 cases per week. The dotted line in the graph represents the target.

The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were created.

Highest Velocity

Represents the owner that currently has the fastest closure rate per week. You can also see the total number of cases assigned to the owner by severity.

The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were assigned to the owner.

Productivity by Owner Groups

Lists the owner groups that currently have the highest average number of cases closed per week. It also identifies which owner in the group has the highest velocity.

You can observe the average number of cases closed and whether the rate is trending up or down. The colored bar indicates the volume of cases by severity. By default, the widget displays data according to the specified time range.

SOAR Productivity

Requires data from ArcSight SOAR.

To help managers optimize analyst activity for the specified time range, the **SOAR Productivity** widget incorporates several elements related to SOC productivity. You can change the widget's properties to select an available option from the **Number of Groups** drop-down list:

Case Closure Velocity

Shows the current rate of case closure per week based on the target velocity for all owners and owner groups. For example, you might expect teams to close at least 5 cases per week. The dotted line in the graph represents the target.

The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were created.

Highest Velocity

Represents the owner that currently has the fastest closure rate per week. You can also see the total number of cases assigned to the owner by severity. The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were assigned to the owner.

Productivity by Owner Groups

Lists the owner groups that currently have the highest average number of cases closed per week. It also identifies which owner in the group has the highest velocity.

You can observe the average number of cases closed and whether the rate is trending up or down. The colored bar indicates the volume of cases by severity.

By default, the widget displays data according to the specified time range.

SOAR Average KPI for Event

Requires data from ArcSight SOAR and that ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

The **SOAR Average KPI For Event** widget provides the SOC Manager an overview for the volume of events in the specified time range that transition from initial analysis of events from source devices through correlation to case creation. The widget also shows the percentage of change between each state.

Correlated Event Count

Shows the number of alerts created from an ESM alert source that you must handle manually, without the use of ArcSight correlation.

Found

Indicates the reduction in the number of items that you must handle manually. This data includes the correlation events generated by rules that monitor events from source devices, as well as events generated by ArcSight components. For typical correlation rule configurations, the data usually represents a reduction in the number of items. However, the number of items might increase in the case of unusual configurations.

Created

Represents the number of cases created within a time range, based on correlation event activity, content, or systems detecting what is significant, and also manual assessments.

SOAR Case Breakdown - Severity

Requires data from ArcSight SOAR.

The **SOAR Case Breakdown - Severity** widget displays the number or percentage of cases by their **Severity**. The widget always shows data **As of Now**, regardless of the specified time range for the dashboard. By default, the widget shows data for total open cases. You can change the widget's properties to select or deselect a severity type. You can also create custom severities. The system, however, does not limit the number of custom severities that you can create.

SOAR Case Load

Requires data from ArcSight SOAR.

To help managers balance the amount of work assigned to case owners, the **SOAR Case Load** widget provides several case management metrics:

- Average number of cases each owner closes per week.
- Projection of the number of cases per severity that the owner might not be able to close, based on the configured target, the time elapsed since the cases were opened, and the average velocity of the owner. This assumes that owners work on cases in severity order, from highest to lowest.

> Estimation of the time required to close all cases is set in the **Severity Editor** when you configure custom severities.

By default, the widget shows the data for total open, assigned cases for the top three members of the group based on their average number of cases per week. You can filter the data by specific Owner Groups. The metrics are based on the specified time range and the target number of cases that you expect the owners to close per Severity

For best use of this widget, it is recommended that you create one Case Load widget per owner group. In this way, you will see details for members of the owner group.

SOAR Case Status

Requires data from ArcSight SOAR.

The **SOAR Case Status** widget displays the number of cases by their Statuses. The widget always shows data **As of Now**, regardless of the specified time range for the dashboard.

By default, the widget shows data for All cases. You can however change the widget's properties to select or deselect one or more Status types.

SOAR Threat Analysis Funnel

Requires data from ArcSight SOAR and that ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

The **SOAR Threat Analysis Funnel** widget provides the SOC Manager an overview for the volume of events in the specified time range that transition from initial analysis of events from source devices through correlation to case creation. The widget also shows the percentage of change between each state.

Analyzed
Shows the number of **events**, from source devices, that you must handle with the use of ArcSight correlation.

Found

Indicates the reduction in the number of items that you must handle manually. This data includes the **correlation events** generated by rules that monitor events from source device as well as events created by ArcSight components. For typical correlation rule configurations, the data usually represents a reduction in the number of items. However, the number of items might increase in the case of unusual configurations.

> Base and Correlation Event counts and Created Case counts come from the *ArcSight ESM* API and *ArcSight SOAR* respectively.

SOAR Case Timeline

Requires data from ArcSight SOAR.

The **SOAR Case Timeline** widget shows changes in the volume of cases over a specified time range. By default, the widget filters the data according to the Severity category assigned in SOAR. However, you can also choose to view trends for other case states, such as cases closed by assigned or unassigned sub-filters.

To observe the breakdown of cases associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

SOAR Top Playbooks Executed

Requires data from ArcSight SOAR.

The **SOAR Top Playbooks Executed** widget displays the execution count of the playbooks over alerts created.

By default, the widget shows data for top 5 playbooks. The widget helps managers understand the count of playbooks executed over each alert.

You can view the number of playbooks for a given date period and Top N Playbooks such as top 5, top 10.

SOAR Trend - Mean Time To Resolve

Requires data from ArcSight SOAR.

The **SOAR Trend - Mean Time to Resolve** widget displays the amount of average time it took to resolve a malicious attack.

You can change the widget's properties to view different classifications of attacks and their statuses.

To observe the breakdown of cases associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

SOAR Trend - Mean Time To Respond

Requires data from ArcSight SOAR.

The **SOAR Trend - Mean Time to Respond** widget displays the amount of average time it took to respond to a malicious attack.

You can change the widget's properties to view different classification of attacks and their statuses.

To observe the breakdown of cases associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

SOAR Trend - Playbooks Executed

Requires data from ArcSight SOAR.

The **SOAR Trend - Playbooks Executed** widget displays the number of times a playbook is executed by its execution date.

By default, the widget shows data for 5 playbooks. The widget helps managers understand the number of playbooks executed everyday.

You can change the widget's properties to view number of playbooks for a given date period.

To observe the breakdown of playbooks associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

Threat Analysis Funnel

Requires ArcSight ESM be deployed. This widget is not available in the ArcSight SaaS environment.

The **Threat Analysis Funnel** provides the SOC Manager an overview for the volume of events in the specified time range that transition from initial analysis of events from source devices through correlation to case creation. The widget also shows the percentage of change between each state.

Analyzed

Shows the number of **events**, from source devices, that would need to be handled manually without the use of ArcSight correlation.

Found

Indicates the reduction in the number of items that you would need to handle manually. This data includes the **correlation events** generated by rules that monitor events from source device as well as events created by ArcSight components. For typical correlation rule configurations, the data usually represents a reduction in the number of items. However, the number of items might increase in the case of unusual configurations.

Created

Represents the number of **cases** created within the time range, based on correlation event activity, content or systems detecting what's significant, and manual assessments.

Top Risky Entities

Requires ArcSight Intelligence be deployed. This widget is not available in the ArcSight SaaS environment.

To help identify the riskiest entities in your organization, the **Top Risky Entities** widget provides a list of the top risky entities, by entity type, based on the last analytics run. By default, the widget displays the top 5 risky users. If you need to view the top risky entities for another entity type, then, as part of this widget's properties, you can change the filter to select the entity type and the number of entities you want displayed in the list. When you click an entity in the widget, the Explore page opens in the ArcSight Intelligence UI, with the selected entity's name applied to the **anomalies and violations** filter.

Searching for 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, as well as view the raw event data. Each search consists of specifying query input, search result fields, and the criteria 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. When running a search, you can specify a fixed time or have the search results update in real-time.

Understanding Search

ArcSight ingests log data, migrated from ArcSight Logger or sent by SmartConnectors directly to the ArcSight Database. Each entry in a log is referred to as an **event**. As the database accepts events, it organizes the data to maximize search and storage efficiency. In a non-SaaS environment, you can configure the SmartConnectors to route events through Transformation Hub and Real-time Threat Detection service in the ArcSight SaaS environment before arriving in the database.

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 enter a search query, the criteria (such as a time window) over which to search, and a fieldset containing the fields from the Unified Event Schema.

For your search, you can use one of the three timestamps that the database stores for each event in your time window. When running a search, you can choose to receive results based on a fixed-time range or stream the results in real time, as events are being ingested. The system treats each search tab as a session search unless you save the search. By default, session searches expire after 24 hours of inactivity. To avoid expiration, save the search as *Search Query*, *Search Criteria* or *Search Results*. You can also schedule searches to run on a regular basis.

> Real-time search is available only with the Real-time Threat Detection service in the ArcSight SaaS environmentt.

When you start a search, the status of the **Search** changes to **In Progress**. Rather than attempting to read all data at once, the search retrieves data in chunks of time and displays

the data in timeline and grid. You can pause search, restart, and cancel the search, as needed.

To help you evaluate the data, Search provides an Event Histogram chart to show the number of events returned over time. The Search Results table shows all events returned based on the current time range of the histogram. The table displays columns of fields for a category of data. When you select an event, you can view its list of field-value pairs in the Event Inspector panel.

> Because search results consume space, the system maintains a threshold for the total number of executed searches that it can store. Stored content includes saved search results, completed runs of session searches, and completed runs of scheduled searches. The system displays a notification when the threshold is passed. If this occurs, you cannot run a search, and scheduled searches cannot run, until some previously executed searches have been deleted.

Understand Fixed-time versus Real-time Searches

Search results can be based on a fixed time range or stream in real time as new events match the search query.

- Fixed-time Searches
- Real-time Searches

Fixed-time Searches

A **fixed-time search** receives results based on a fixed time range, such as having fixed start and end values. For example, 10:00 AM to 10:00 PM on May 29. The search also can use dynamic dates, such as last 30 minutes or the last 24 hours. However, after the system retrieves the search results, Search does not update the dataset again. To receive more recent events, you might have to reconfigure the end time if using specific end time and re-run the search.

Real-time Searches

A **real-time search** constantly updates the results of your query, starting from a beginning range, such as **Last 30 Minutes**. As long as there is data to satisfy the query, the data in the Events Table continues to build. Real-time search requires the *Real-time Threat Detection* service in the ArcSight SaaS environment.

Real-time searches act like session searches; their expiration time depends upon what you have in user preferences for "Session Search expires in" when the real-time search was created.

Options for creating searches:

- Create a Fixed-time Search
- Create a Real-time Search

Understand Session Search versus Saved Search Results

The system enables you to initiate temporary searches, as well as save searches to run again. The Home tab lists all your current searches. Therefore, if you close the search tabs or lose the search tabs by logging out, you can open them again from the Home tab. However, if the search results have expired, you cannot re-open the search.

- Session Searches
- Saved Search Results
- Expired Searches
- User Activity With Real-time Searches

Session Searches

As you initiate a search, your activity is automatically preserved in case you need to navigate to another search tab or to a different feature in the ArcSight Platform. Search temporarily maintains these **session searches** after you close the search tabs, exit your browser, or log out. The system might automatically log you out if you have not interacted with the interface for longer than an idle time specified by your system administrator.

The session search expires once the specified expiration time is reached, regardless of the level of activity in the session.

Saved Search Results

For long-term use of a search, you must save the query, criteria, or results. Note that, for a real-time search, you cannot save the query. You can review and manage your **saved searches** at any time:

- Saved queries
- Saved criteria
- Saved search results

Expired Searches

Session and saved searches usually **expire** after a specified amount of time.

When a search expires, the system deletes all information about the search. If this occurs when you have the search open in a tab, you will receive a notification that the search has expired and be instructed to close the tab.

The session search expires once the specified expiration time is reached, regardless of the level of activity in the session. You may reset the expiration time by running the search again or by modifying the query or criteria. However, if the search has already expired, you cannot reset the expiration clock. You can also override the default expiration time by changing the **Search expires in** setting for a particular session search.

By default, search results expire after seven days. (You may modify this value in your user preferences.)

User Activity With Real-time Searches

After a certain number of minutes, the application will log you out and redirect you to a Login page if the system does not detect any user activity in an open search tab that contains a running real-time search.

To avoid the logout behavior, you can request your system administrator to activate the **Never Expire Session for Real-Time Searches** permission. This allows the user to leave a running real-time search opened in a tab and prevents the logout if there is no interaction with the user interface. User interface activities include scrolling, mouse movements, mouse drags, clicks, zooming in or out, and keystrokes.

Understand Search Limits for Fixed-time Searches

For fixed-time searches, if you exceed the search limit, the system displays an error message when you create a new search: *An error occurred while creating search. Exceeding the limit of 1000 searches*. You cannot create more searches if this error displays.

Contact your Administrator to increase the search limit or delete some existing searches. For more information about increasing the search limit in a non-SaaS environment, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform 23.3*. If you are an ArcSight SaaS customer, reach out to Support to increase the search limit.

Understand Search Limits and Start Times for Real-time Searches

Requires the Real-time Threat Detection service in the ArcSight SaaS environment.

The following sections provide a deeper discussion about how the start time of a real time search histogram is calculated, what happens when a real time search reaches its search results limit and go to now behavior.

- Understand Start Time of the Histogram

- If Search Reaches the Search Results Limit

- Understand Go-to-Now Behavior

Understand Start Time of the Histogram

To find events that match the query, Search needs a time range, particularly a starting time. If you selected a time range of **Last 1 hour** and began the search at 8 am, the initial time range for the search will be from 7 to 8 am.

If you create a real-time search with the **Do not accumulate data** option as time proceeds and data continues to be added, the start time of histogram time window also continues to move forward. For example, if 30 minutes has passed since you created real time search at 8 am, the histogram will show data for 7:30 am to 8:30 am.

> The **Do not accumulate data** option only pertains to histogram display. Data will continue to accumulate in the backend. You can always pan backward to see the older data.

If you had deselected **Do not accumulate data** when you created your real-time search, the histogram will show all of the data from the time you created the search. Therefore, if you created the search at 8 am and selected **Last 1 hour**, at 8:30 am, the histogram will show data from 7 am to 8:30 am.

If Search Reaches the Search Results Limit

The start time never changes if your search does not reach the search results limit. Once a real-time search reaches the search limit, the oldest events are dropped to make space for the new events.

Since the oldest events are dropped, the system now sets the start time based on the earliest events that are available in the search results table. For example, if the search limit was reached at 6 pm and system has dropped some events; even though the initial start time was 7 am, if the earliest data present in search results table is now for 8:45 am, the histogram shows data for 8:45 am to 6 pm (assuming **Do not accumulate data** was unchecked). If this option was selected, the histogram will display data for 5 pm to 6 pm, but you can only pan backwards to 8:45 am, not the initial 7 am.

Understand Go-to-Now Behavior

For real-time searches, **Now** is always the present time, which continues to change as the time of day progresses. If you select a start time of **Last 1 hour** and begin the search at 8 am, the **Now** time will change as the search progresses. Therefore, if you pause the search for 1.5 hours and then click the ⊘ icon (only available for real-time searches), the **Now** time becomes 9:30 am.

The beginning of your time range is indicated by a vertical dotted line topped by a solid circle. **Now** or the end of the time range is indicated by a vertical dotted line topped by the ⊘ icon.

Understand Search Queries

You must have the **Manage Search Queries** *permission.*

A **search query** is a set of conditions used to select events when you run a search. For example, you can enter a very simple term to match such as "login" or an IP address. Alternatively, you can specify a complex query to match events that include multiple IP addresses and reference a lookup list. In the search query, you can enter the alias, or abbreviated term, for a field name rather than entering the full name. You can also use the **presentable field names**, such as Agent Address.

Your query input determines the search type: full text, natural language, or contextual. As you specify the fields and values for the query, Search suggests search items and operators based on a schema data dictionary.

Search provides default queries, labeled as *system*. However, you can save your own queries, which you can load into another search. You have the option to clone, modify, or remove a saved query at any time.

Understand the Query Syntax

Depending on the type of search you create, your query must meet the requirements listed in the following table. Search treats a comma (,) between search items and values as an **OR** operator. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query.

If you do not get the search results you expect, you might need to restate the query. For example, if the query is written with spaces, only the first word is shown in the results. A better way to write the query statement is to use explicit phrasing without any spaces.

By default, search operations are case-sensitive to support faster performance. However, you can instruct the database to support case-insensitive searches. For SaaS deployments,

talk to your SaaS Admin about changing the database. For non-SaaS deployments, see the *Administrator's Guide to ArcSight Platform 23.3*.

When you construct a query, you can include operators, such as eval and lookup, for more robust searches.

> You cannot use multiple operators, such as *NN* and *XX*, in the same query.

- General Syntax Rules
- Implicit Operators

General Syntax Rules

Type	Full-text	Field-based	Hashtag (predefined)
Case sensitivity	Case-sensitive	Case-sensitive	Case-insensitive
Exact Match	Keyword treated as keyword*. Example: /Execute matches: /Execute, /Execute/Start, /Execute/Response,/Execute/Query	Enclose value in double quotes. Example: `Category Behavior ="/Execute"`	n/a
Nesting, including parenthetical clauses, such as (a OR b) AND c	Allowed Use boolean operators to connect and nest keywords.	Allowed Use boolean operators to connect and nest keywords.	Allowed Use boolean operators to connect and nest keywords.
Implicit Operators	When you enter two values separated by a space, this is treated as an implicit AND condition. Example: `ssh fail`	The AND/OR treatment depends on the operator used in the search. 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 , 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.	n/a
		*Syntax for an Inner Join:*source address in list CustomListName_CustomColumn Name	
		*Syntax for a Left Join:*source address not in list CustomListName_ CustomColumnName	
Time Format (when searching for events that occurred at a particular time)	No specific format The query needs to contain the exact timestamp string. Example: "10:34:35"	YYYY-MM-DD YYYY-MM-DD HH:mm YYYY-MM-DD HH:mm:ss.fff To narrow the time range, use the following operators: • in between (><) • greater than (>) • less than (<)	n/a
Special Characters: \ * ' "	Use the backslash (\) as an escape character.	Use the backslash (\) as an escape character.	n/a
Wildcard	Can appear anywhere in the value. Examples: *log log* lo*g* Searches for ablog, blog, long, etc.	Can appear anywhere in the field. Examples: name=*log Searches for ablog, blog, etc. in name field name="*log" name=*log Both search for *log	n/a
Escape a Wildcard Character	Can search for * by escaping the character. Example: log*	Can search for * by escaping the character. Example: log*	n/a

Implicit Operators

Implicit operators form the basic building blocks for query construction. Use them along with other operators and functions to create robust search queries.

To build queries, use the following general operators:

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

does not contain	does not have	name does not contain TCP
in list	match in list of	device vendor equals CISCO and source address in list customListName_ customColumnName device vendor equals CISCO and source address in list badGuyIpList_badGuyIp
not in list	not match not in list of	source address not in list customListName_customColumnName source address not in list badGuyIpList_ badGuyIp
in subnet	n/a	source address in subnet 10.0.0.0/8
not in subnet	n/a	source address not in subnet 10.0.0.0/8

Understand the Types of Search Queries

Search supports the following types of search queries:

- Full Text Search

- Field-based Search

- Hashtag (predefined searches)

Full Text Search

Searches across all fields using a 'contains' operation to determine if the value is found.

Syntax	Example
<value>	ssh

Field-based Search

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

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

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

Hashtag (predefined searches)

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

To ensure the system correctly parses your query, if your search entity name includes one of the reserved words listed before, you should surround the query name with quotes (" ") in order to avoid ambiguity in the query statement.

This predefined query...	Description
#Configuration Changes	Lists configuration changes based on ArcSight categorization.
#DGA Events	Lists DGA-related events based on Microsoft Trace Log.
#DNS Events	Lists DNS-related events.
#DoS Events	Lists events indicating denial of service based on ArcSight categorization.
#ESM Correlation Events	Lists ESM correlation events.
#Failed Logins	Lists events indicating failed login activity based on ArcSight categorization.
#Failed Logins For User $Username	Lists events indicating failed login activity based on ArcSight categorization for a specific user. The user should be specified before running the search.
#Firewall Drop	Lists Drop Firewall events based on Arcsight categorization for a specific IP address. The IP address should be provided at runtime.
#Firewall Drop For $Ip	Lists Drop Firewall events based on Arcsight categorization.
#Firewall Events	Lists Firewall events based on ArcSight categorization.
#Malicious Code Activity	Lists events indicating malicious code activity based on ArcSight categorization.
#MITRE ATT&CK Events	Lists correlation events reported from Arcsight ESM content package: https://marketplace.microfocus.com/cyberres/content/esm-default-content. These events are forwarded to the ArcSight Database using ArcSight Forwarding connector, or any other flex connector which reports this information, using the following mapping: deviceCustomString6Label='MITRE ID' Where deviceCustomString6 contains the actual MITRE ATT&CK technique.
#Proxy Events	Lists Proxy events based on ArcSight categorization.
#SSH Authentication	Lists events indicating SSH Authentication events based on ArcSight categorization.
#VPN Connections	Lists events indicating VPN connections based on ArcSight Categorization.

#Vulnerabilities Events	Lists events indicating vulnerabilities based on ArcSight categorization and Vulnerability Scanner events.
#Windows Account Creation	Lists events indicating new windows accounts created based on the following event sources: • Microsoft-Windows-Security-Auditing:4720 • Security:624
#Windows New Service Created	Lists events indicating new windows services were created from the following event sources: • Microsoft-Windows-Security-Auditing:4697 • Service Control Manager: 7045

Use Reserved Words in a Query

To ensure the system correctly parses your query, if your search entity name includes one of the reserved words listed before, you should surround the query name with quotes (" ") in order to avoid ambiguity in the query statement.

For example, if your query name is: "System warnings and errors" use the following notation: #"System warnings and errors."

Reserved Words for Queries		
and	as	between
by	category	connecting to
contain	contains	custom float
distinct	does not contain	does not end with
does not start and end with	domain	ends with
endswith	equal	equals
filter	for	greater
greater equal	greater equal than	greater than
gte	has	has substring
hostname	ibt	id
in between	in cidr block	in list
in list of	in subnet	is
is between	is equal	is equal to
is greater	is greater or equal than	is greater than

Reserved Words for Queries		
is greater than or equal to	is larger	is larger than
is less	is less equal	is less or equal than
is less than	is less than or equal to	is lower
is lower than	is not	is not between
is not equal	is not equal to	ip
ip6	label	less
less equal	less equal than	less than
like	lte	mac
match	nibt	not
not between	not equal	not equals
not in between	not in cidr block	not in list
not in subnet	not match	not within subnet
or	path	pipe
port	span	starts and ends with
starts with	startswith	timestamp
username	uri	url
where	wheresql	within subnet
withinsubnet		

Include a Storage Group's Filter in the Search Query

Search allows you to include a storage group in a query so that you can search for events only in that group. 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.

Use GlobalEventID in a Query

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

Syntax	Example
global event id=<value>	global event id= 2864991913017849867

For events to have a GEID, use ArcSight Management Center to configure connectors to include the ID. For more information in:

- Non-SaaS environments, see "Generator ID Manager" in the *Administrator's Guide to ArcSight Platform 23.3*.
- SaaS environments, see " Setting Up Generator ID Management" in the *Quick Start for Administrators*.
- SmartConnectors, see "Unique Generator ID" in the *ArcSight SmartConnector Installation Guide*.

Specify an Alias for a Field

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

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

Field	Aliases
categoryBehavior	behavior
categoryDeviceGroup	device group
categoryObject	object
categorySignificance	significance
categoryTechnique	technique
destinationAddress	dst
	destination ip
	destinationip
	dst ip
	dest ip
	target ip
	targetip
	target
destinationHostName	dhost
	destination name
destinationMacAddress	dmac
	destination mac
destinationNtDomain	dntdom
destinationPort	dpt
	destination port
	dstport
	dest port
	targetport
	target port
destinationProcessId	dpid
destinationProcessName	dproc
destinationTranslatedAddress	destination translated ip
destinationuserId	duid

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

Field	Aliases
deviceEventCategory	cat
deviceHostName	dvchost
deviceMacAddress	dvcmac
	device mac
deviceProcessId	dvcpid
deviceReceiptTime	rt
deviceTimeZone	dtz
deviceTranslatedAddress	device translated ip
endTime	end
eventOutcome	outcome
fileNme	fname
fileSize	fsize
message	msg
requestUrl	request
	URL
sourceAddress	src
	source ip
	sourceip
	src ip
sourceHostName	shost
sourceMacAddress	smac
	source mac
sourceNtDomain	sntdomain
sourcePort	spt
	srcport
	src port
sourceProcessId	spid
sourceProcessName	sproc
sourceTranslatedAddress	source translated ip
sourceUserId	suid

Field	Aliases
sourceuserName	suser
	src user
	source user
	src usr
sourceUserPrivileges	spriv
startTime	start
transportProtocol	proto

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 field associated with the group. The following table provides some common group aliases.

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

Specify IP Addresses and Subnets

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

Compare IP addresses for optimum performance
> For example, `Agent Address > 192.10.11.12`.

Specify a range of IP addresses
> For example, you can enter the following types of queries:
> - `Agent Address in between 192.2.13.1 and 192.2.13.11`
> - `Source Address greater equal than 192.10.11.12`
> - `Destination Address less than 192.112.98.33`

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.

To enter an IP or MAC address in a search query:

Enter the MAC addresses in the following formats:
- aa:aa:aa:aa:aa:aa
- aa-aa-aa-aa-aa-aa

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

Type of address	Format in a query...	Examples
IPv4	a.b.c.d	a.* a.b.* a.b.c.* a.b.c.d/8
IPv6	Full form	2001:0db8:0000:0000:0000:ff00:0042:8329
	Canonical form without leading zeroes in each group	2001:db8:0:0:0:ff00:42:8329
	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 2001:0db8:0000:0000:0000:ff00:0042:8329/24 2001:db8::/32 **NOTE**: For the 2001:db8::/32 format, you can omit part of the IPv6 address, depending on the subnet that you are querying.
MAC	a:b:c:d:e:f a-b-c-d-e-f	94:18:82:6D:63:74 94-18-82-6D-63-74

Use an Operator in the Query

Create powerful queries with search operators and functions. You can also select several out-of-the-box system searches that contain a query plus specific criteria. Operators, such as eval, can be chained together to create complex queries.

> Search operators and functions must be entered in all lower case letters when they are used in queries.

> Do not use a raw event field as part of a query.

Use Cases for Search Operators

The following are just a few examples of the flexibility and power of search operators.

- General Search Operator Use Cases
- Operator Chaining Use Cases

You may need to adjust a query to work with your own fieldsets.

For more information about working with operator chaining see Use an Operator in the Query and Chaining Search Operators.

General Search Operator Use Cases

I want to see where possible brute force password guessing is happening.

Additional Information: To determine this, I want to see the top 10 devices that are responsible for the most number of failed logins.
Operator used: top

```
#FailedLogin | top 10 deviceEventClassId
```

I want to know the hourly amount of data transfer on MyWebserver.

Operators used: chart, sum, by, span

```
sourcehostname = MyWebserver.com | chart sum(bytesIn), sum(bytesOut) by
deviceVendor, deviceProduct span 1h
```

I want to see a sum of events, grouped by hostname and day.

Operator used: chart
Aggregate function: sum (This summarizes the values passed as an input, grouped by the "by" clause.)
Time bucket: 1h (Events are grouped in time increments of one hour.)

```
| chart sum(baseEvents) by hostName span 1h
```

I want to determine all account lockouts, grouped by user name.

Operators used: wheresql, top

```
(deviceVendor="Microsoft" and deviceProduct="Microsoft Windows") or
deviceProduct="Unix" | wheresql  deviceEventClassId in
["Security:539","Security:644","arcsight:66:0","Microsoft-Windows-
Security-Auditing:4740","Microsoft-Windows-Security-Auditing:6279"] and
 destinationUserName is not null |top destinationUserName
```

Operator Chaining Use Cases

I want to identify the rare occurrences of Firewall events.

Additional Information: I want to determine this from 3 specific fields' data (device vendor, category device group, and name).
Operators used: rename, rare (bottom)

```
#Firewall Events | rename deviceVendor as DV | rename category device
group as CDG | rare DV , name , CDG
```

I want to isolate vulnerabilities.

Additional Information: I will base this on data from 3 significant fields (device vendor, category technique, and device group), then determine the most common occurrences found in those categories.
Operators used: rename, rare (bottom)

```
#Vulnerabilities | rename deviceVendor as DV | rename category
technique as CT | rename category device group as CDG | rare DV , name
, CDG , CT
```

I want to apply filters to a set of fields and then to extract the top-50 most common occurrences of those events.

Operators used: where, top

```
source address is not null | where Bytes In >= 3000 | where Category
Outcome = /Success | top 50 source address , Category Outcome
```

I want to determine the top insecure processes on devices in my company.

Operators used: top, rename

```
destinationProcessName in ["telnetd", "ftpd", "pop3", "rsh" ,
"imapd","rexec"] | top destinationProcessName  | rename
destinationProcessName as  "Process"
```

```
deviceVendor = ArcSight | rename sourceUserName USER | top USER
```

Show me all configuration changes by product.

Operators used: top, rename

```
categoryBehavior = "/Modify/Configuration" and categoryOutcome =
"/Success" | top deviceProduct | rename deviceProduct_count_2 as
"Changes" | rename deviceProduct as "Product"
```

I want to apply filters to a set of fields and then to extract the top-50 most common occurrences of those events.

Operators used: where, top

```
source address is not null | where Bytes In >= 3000 | where Category
Outcome = /Success | top 50 source address , Category Outcome
```

Chaining Search Operators

Construct a complex query statement by chaining together multiple search operators into a single query instead of implementing separate queries. This powerful capability lets you perform robust, real-world searches while providing the flexibility to customize searches for specific scenarios. You can save these searches to reuse them in future updates.

Operator chaining is a process by which the search takes a set of results from one operation and uses these results as input for the next operation. Chaining a series of operations equips you with the options needed to "slice and dice" data to extract and analyze it on a highly granular level. Operator chaining works with all the pipeline operators (rename, eval, where/filter, wheresql, top, bottom/rare and chart/stats). The number of search operators supported in a particular query might vary, based on your database configuration and load.

During operator chaining, fieldsets become more restricted as more operators are added to the query, especially with eval and aggregation operators. For example:

```
severity!=null | top severity | stats avg (Count_1) by severity
```

For information about operator chaining workflows, see Use Cases for Search Operators.

Syntax Recommendations

Use the following syntax recommendations to ensure operator chained searches succeed.

- To use the fields from a **lookup list** table with the search operators, make a **join** with one of the lookup fields using the **"in list"** operator. You also should add the lookup list fields to the current fieldset. For example:

  Add a lookup list with name as **Customer** then add its field, which will be used with

search operator (e.g. **Customer_Vendor**) to the current fieldset.

```
Source Address in list Customer_Address | wheresql Customer_Vendor =
'Microsoft'
```

- **Alias/New** field name cannot be an existing field name or a synonym of an existing field name. Also, an alias field name cannot be an existing group name or reserved word.

  In this example, "destination hostname" and its synonyms "dhost" and "destination name" cannot be used as aliases.

- **Alias/New** field name should not have spaces (like test 1), otherwise it will cause conflicts. These are examples for acceptable alias/new field names:

```
name is not null| eval test1 = concat(name, "_test") | eval test_2 =
upper(test1)
```

```
name is not null | where name not equals ARCSIGHT | chart count
(distinct name) as Dcount by name
```

- For all pipeline operators, special characters used in aliases have syntax restrictions. This includes those described in the eval, chart and stats, rename, top and bottom, and where operators.

- The following is an example of how to use a generated field with **eval** in another operator:

```
| eval test = upper ( name ) | where test != "ARCSIGHT"
```

- **Count_<number>** cannot be used as an alias for a field name.

- The **wheresql** operator is case sensitive. Just like all other operators, the wheresql name must be stated in all lower case letters.

- Do not create new field name with spaces if these new fields will be used later with the **wheresql** operator. The where condition of wheresql operator will not recognize new field with spaces that were created by previous operators. In addition to wheresql, this is also applicable for the **eval** and **chart and stats** operators. Here are two **invalid** examples:

```
| rename name as new name | wheresql new name = 'TCP'
```

```
destination port is not null | eval convert name = upper ( Name ) |
wheresql convert name = 'MSTYPE'
```

- You can use the **where** operator to filter dynamic fields, for example:

```
| top 5 Name | where Count_1 > 1000
```

- More filters can be added to a search through the Fields Summary feature. Click on **Fields Summary** and select a field and a value for that field. The new filter will be appended at the end of the query in use as a |**where** clause.

- Multiple **aggregate functions** can drastically modify drastically the fieldset that is available for the next pipe operator. for example:

```
name is not null | char count (Name) by Device Vendor span 1h | chart
count (Name) by Name
```

The second chart pipe cannot access to span operations because the NET, DRT, dBRT are not available for this chaining level.

Same scenario applies to the **top** operator:

```
name is not null | top Name | char count(count_Name_1) by Name span
1h
```

chart/stats

The **chart/stats** operators display search results for specified fields as fields in the Search Results table.

- Syntax
- Aggregation Functions
- The Span Function
- How Do I Use This?

Syntax

```
...| chart count by field1, field2, field3 ... [span [time_field]=time_
bucket]
...| chart {{sum | avg | min | max | } (field)}+ by field1, field2, field3
...[span [time_field]= time_bucket]
...| chart {function (field)} as new_field_name by field [span [time_
field]
```

For simple syntax examples, see below.

where:

- *field*, *field1*, *field2* are the names of event fields used in system queries.
- *time_bucket* is the bucket size (in any combination) used for grouping events. Use **d** for day, **h** for hour, **m** for minute, and **s** for seconds. For example, *2h*, *5d*, *1m*.
- *function* is one of the following: **count, sum, avg , min, max, latest** or **earliest**..
- *new_field_name* is the name you want to assign to the field (field of data) in which the function's results are displayed. For example, *Total*.
- All chart/stats commands accept only one field in the input. For example, | stats count (device vendor) by...
- The input field must contain a field that exists in the database.
- If multiple fields are specified, separate the field names using commas without any spaces.
- The function input field must contain numeric values for chart/stats sub-operators that are mathematical operations (sum, avg, min, max).
- The mathematical operators **avg** and **mean** are equivalent.

"by" Statements

- The chart/stats operators and eval, require a "by" statement. For example: eval | chart sum(AgentSeverity) by Destination HostName
- Specify a field name after the "by" statement. For example: "by deviceVendor"
- Fields in a "by" statement should be separated by comma. For example: ... | chart count(Name) by deviceEventCategory , name

Simple Syntax Examples

- Grouping events by a field and counts how many names each group has.

```
...| chart count(name) by Destination Hostname
```

- Sum of Bytes In for every group of events. These events (rows) are grouped by the field Destination Hostname.

```
...| chart count(Bytes In) by Destination Hostname
```

- The events (rows) are grouped using the default time field selected, distributing the events in groups of 1 hour. The events that matches the same time bucket and the same Agent Severity will be organized in the same group. Then returns how many names contains every group.

```
...| chart sum(name) by Agent Severity span = 1h
```

Aggregation Functions

> Aggregation functions only work on numeric fields. The specified fields must contain numeric values. If a field you specify is of the wrong data type, you will receive an error message like the following: "java.lang.NumberFormatException".

- You can include multiple functions in the same chart/stats command. When doing so, separate each function with a comma, as shown:

-
```
... | chart count (Name) by Destination Hostname, sum
(deviceCustomNumber3) by deviceEventClassId
```

- When you include multiple functions, the search results table displays one field per function.
- You can use the "**as new_field_name**" clause to name any field resulting from the aggregation functions, as shown:

```
...| chart sum(deviceCustomNumber3) as TotalStorage, avg
(deviceCustomNumber3) as AverageStorage by deviceCustomNumber3
```

- Instances of "**new_field_name**" should be changed by the alias name of the aggregation result.

Aliases that contain special characters have the following syntax restrictions:

Special Characters	Restrictions	Examples
+, *, &, - , = , <, >, |	Need to be enclosed in single/double quotes when they are reused and the search works as expected.	| rename file path as 'FP+DEV' | chart count ('FP+DEV') by 'FP+DEV'
@, #, +, ?, /, ^, [], {}, _ , *, ~	Do not need to be enclosed in single/double quotes when they are reused and the search runs as expected.	| rename file path as 'FP$DEV' \| chart count (FP$DEV) by FP$DEV

The Span Function

In addition to grouping events defined by **eval** operators, the **span** function groups events by a time field (such as EventTime or deviceReceiptTime) and a time bucket.

- The span function can only accept three fields (Normalized Event Time, Device Receipt Time, and Database Receipt Time) before the equals sign, for example:

  - |chart sum(Agent Severity) by Destination hostName span Normalized Receipt Time = 1h

  - |chart sum(Agent Severity) by Destination hostName span = 1h

- |chart sum(Agent Severity) by Destination hostName span 1h

- The span operator is not allowed after an aggregation operator.
- The span operator must use an equal sign or a supported field name. For example: span Normalized Event Time = 1h
- The span operator only accepts timestamp fields. For example: span Normalized Event Time = 1h.
- A span's time bucket must use one of the following types of values: *number*d, *number*h, *number*m, and *number*s

- By default, the chart/stats command displays the first 10 unique values. If the span function creates more than 10 unique groups, not all of them will be displayed.
- When span is included in a query, search results are grouped by the specified time bucket. For example, if span=5m, the search results will contain one row for each 5-minute span. If there are no events within a specific 5-minute span, that row will be empty.

- The span function assumes a **24-hour day, all year long**. If span=1d or 24h, on the day of the daylight savings time change, the event time indicated by the span_eventTime field in the search results will be different from the previous day by one hour. On the day when there are 23 hours in a day (in March), the span bucket will still include events from the last 24 hours. Similarly, on the day when there are 25 hours in the day (in November), the span bucket will include events from the last 24 hours.

How Do I Use This?

Aggregation Function Examples
- Use the default chart setting (Column Chart) to specify multiple fields. In this example, a count of unique groups of deviceEventCategory and name fields is displayed and plotted.

```
... | chart count(Name) by deviceEventCategory name
```

- Simple query using 1 (min) aggregation function and one group by field (min)

```
... | [chart | stats] aggregation_function (field_name) [as alias_
name] by field_name
```

```
 chart count (Name) by Destination Hostname
```

- Query using 1 to *N* aggregation functions, the result and 1 to *N* group by field (min)

```
... | [chart | stats] [aggregation_function (field_name), ...
```

```
aggregation_function (field_name)] [as alias_name] by field_name
```

```
chart count (Name), sum(Agent severity) by Destination Hostname
```

- Query using 1 to *N* aggregation functions, the result and 1 to *N* group by field (min)

```
... | [chart | stats] [ aggregation_function (field_name), ...
aggregation_function (field_name)] [as alias_name] by field_name [,
...field_name]
```

```
chart count (Name), sum(Agent severity) by Destination Hostname, Name
```

- Adding alias in every aggregation function

```
... | [chart | stats] [ aggregation_function (field_name), ...
aggregation_function (field_name)] [as alias_name] by field_name [,
...field_name ]
```

```
chart count (Name) as alias_name1, sum(Agent severity) as alias_name2
by Destination Hostname, Name
```

Span Function Examples

- If time stamp is specified for span input, it does not use parenthesis: The correct query would be:

```
...| chart count(Name) by deviceEventCategory span deviceReceiptTime
= 5m
```

- Destination Hostname is the time field and one hour is the time bucket:

```
  chart count (Name), sum(Agent severity) by Destination Hostname,
Name span 1h
```

- deviceReceiptTime is the time field and 5m (5 minutes) is the time bucket:

```
...| chart count(Name) by deviceEventCategory span
(deviceReceiptTime) = 5m
```

- Span is used to organize events by time frame:

```
... | [chart | stats] [ aggregation_function (field_name), ...
aggregation_function (field_name)] [as alias_name] by field_name [,
... field_name ] span = n[s|m|h|d]|m|h|d]
```

- If a time field is not specified for the span function , EventTime is used as the default.

For example, the following query uses EventTime by default:

```
...| chart count(Name) by deviceEventCategory span = 5m
```

Grouping with span is useful in situations when you want to find out the number of occurrences in a specific time span.

- If you want to find out the total number of incoming bytes every 5 minutes on a device, you can specify a span of 5m. This example assumes that deviceCustomNumber1 field provides the incoming bytes information for these events.

```
...| chart sum(deviceCustomNumber1) by hostName span 5m
```

- You want to see a sum of events by hostName in one week of events, listed by day. When a **span** field is specified in conjunction with an **event** field, the unique sets of all those fields are used for grouping.

```
...| chart sum (baseEvents) by hostName span = 1d
```

- The following example uses deviceCustomNumber and deviceAddress in conjunction with span to find out the number of events (using deviceCustomNumber3) from a specific source (using deviceAddress) in one (1) hour:

```
...| chart sum(deviceCustomNumber3) by deviceAddress span=1h
```

- When span is included in a query, search results are grouped by the specified time bucket. For example, if span=5m, the search results will contain one row for each 5-minute span. If there are no events within a specific 5-minute span, that row will be empty.

- The span function assumes a **24-hour day, all year long**. If span=1d or 24h, on the day of the daylight savings time change, the event time indicated by the *span_eventTime field* in the search results will be different from the previous day by one hour. On the day when there are 23 hours in a day (in March), the span bucket will still include events from the last 24 hours. Similarly, on the day when there are 25 hours in the day (in November), the span bucket will include events from the last 24 hours.

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

rename

Use the pipeline operator **rename** to assign a new name to a portion of the search query.

- Syntax

- How Do I Use This?

Syntax

```
... | rename source_name as new_source_name
```

where

- *source_name* represents the field that you want to rename.

- *new_source_name* represents the new name that you want to apply to the field.

Aliases that contain special characters have the following syntax restrictions:

Special Characters	Restrictions	Examples
@, #, +, ?, /, ^, [], {}, _ , * , ~	Do not need to be enclosed in single/double quotes when they are reused and the search runs as expected.	| rename source address as 'source@' | rename source@ as SA
&, !, - , = , <, >, |	Need to be enclosed in single/double quotes when they are reused and the search works as expected.	| rename source address as 'source&' | rename 'source&' as SA

How Do I Use This?

- Assign a new address name to an existing source address.

```
... | rename source_address as SourceAddressABC
```

For more information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

top and bottom

The **top** and **bottom** operators list the search results of the most common values for the specified field. The resulting values are listed in tabular format from the highest count value to the lowest.

The fields can be event fields, available in the application menu. If multiple fields are specified, you need to separate the field names with white space or a comma.

As a convenience, top and bottom operators are included in out-of-the-box system searches. These system searches contain a query plus specific criteria.

- [top](#)
- [bottom](#)
- [Syntax](#)
- [Parameters](#)
- [How Do I Use This?](#)

top

The **top** operator provides the most common values for the specified field(s). The values are listed from the highest count value to the lowest.

bottom

The **bottom** operator provides the least common values for the specified field(s). The values are listed from the lowest count value to the highest. The **rare** operator can be used as an alias to **bottom**.

Syntax

```
…| top [N] field1 [,field2, field3]
```

where:

- [ ] indicates optional input you may enter.
- Italicized characters indicate where a user can enter *custom* [field](#) information.
- Only *N* is optional. *N* limits the matches to the top *n* values for the specified fields. One (1) field is required, but you can specify a maximum of five (5) integers, separated by commands.
- If you do not specify *N*, the default value is 500.
- If included, *N* should be between one (1) and the search results limit.
- The operator performs a standard count (*) to retrieve the number of events.
- No search operator other than "where" can be used in a query after the top/bottom operator is used.
- Queries that use the top/bottom search operator along with fields that begin with "Device" may fail completely or partially. To avoid this behavior, select the field from the drop-down options that are available as you enter the query. This also applies to fields that are not editable.
- Aliases that contain special characters have the following syntax restrictions:

Special Characters	Restrictions	Examples
*, -	Do not need to be enclosed in single/double quotes when they are reused and the search works as expected.	Destination port <> null | rename Destination Port as 'D*P' | rename Source Port as 'S*P' | top 10 D*P , S*P
@, #, ?, /, ^, [], {}, _ , *, ~	Do not need to be enclosed in single/double quotes when they are reused and the search works as expected.	Destination port <> null | rename Destination Port as 'D#P' | top D#P

Parameters

The parameters are *N* and a list of comma-separated fields.

For the **top** operator, when multiple fields are specified, the count of unique sets for all of the fields is listed from the highest to lowest count. For the **bottom** operator, the fields are listed from the lowest to the highest count.

How Do I Use This?

The top operator is used to limit the matches to the top *N* values for the specified fields. Likewise, the bottom operator is used to limit the matches to the bottom *N* values for the specified fields. The default count number is 500 unless you specify a value for *N*. Here are a few examples:

- You want to limit your results to the 1,000 most common event categories.

```
…| top 1000 deviceEventCategory
```

- You want to limit your search for the top 5 event categories.

```
…| top 5 categories
```

- You want to see all products from a specific vendor that are sending the least number of events.

```
deviceVendor = Vendor| bottom 10 deviceProduct
```

- See the "rare" user action in the organization happening using the HTTPS protocol.

```
protocol=https | rare requestuseragent
```

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

where

The **where** operator displays events that match criteria specified in a "where" expression. Where expressions act as filters to return only those results that fulfill a particular condition. In fact, **filter** is a synonym of the operator **where**. Results for where expressions are binary, satisfying either true or false.

- Syntax

- How Do I Use This?

Syntax

```
... | where <expression>
```

where:

- The *where* operator represents the filter you want to use us on a field.

- The *expression*field represents a valid field-based query expression. Arithmetic expressions or functions are not supported.

- For *where any … contains* queries, all fields are executed, but only results for alpha (letter) IDs are displayed. For example, results for the ID "HostName" display, but results for the ID CEID-3631 will not display, even though the field is executed.

- You can specify multiple field conditions in one query expression by using the listed operators between them. The conditions can also be nested. For example:

  ```
  (name="John Doe" OR name="Jane Smith")AND message!="success"
  ```

- Aliases that contain special characters have the following syntax restrictions:

Special Characters	Restrictions	Examples
@, #, +, ?, /, ^, [], {}, _ , *, ~	Do need to be enclosed in single/double quotes when they are reused and the search works as expected.	| rename source address as 'source@' | where source@ <> null
&, !, - , =, < , >, |	Need to be enclosed in single/double quotes when they are reused and the search works as expected.	| rename source address as 'source&' | where 'source&' <> null

How Do I Use This?

```
... | where eventId is NULL
```

```
... | where eventId=10006093313 OR deviceVersion CONTAINS "4.0.6.4924.1"
```

```
... | where eventId >=10005985569 OR categories= "/Agent/Started"
```

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

wheresql

The wheresql operator displays events that match criteria specified in a boolean expression (satisfying either true or false). These expressions act as filters to return only those results that fulfill a particular condition. You can use the Eval functions listed in this guide in wheresql expressions. Database SQL functions that can be used in a Where clause of an SQL query can also be used in wheresql operator expressions. This allows you to construct powerful queries.

For example, to detect plain text credit card information in events, you can create the query:

```
| wheresql regexp_ilike(deviceCustomString1,
'^(?:4[0-9]{12}(?:[0-9]{3})?|[25][1-7][0-9]{14}|6(?:011|5[0-9][0-9])[0-9]
{12}|3[47][0-9]{13}|3(?:0[0-5]|[68][0-9])[0-9]{11}|(?:2131|1800|35\d{3})\d
{11})$')
```

- Syntax
- Parameters
- How Do I Use This?

Syntax

```
…|wheresql boolean_expression
```

Wheresql expressions are binary, satisfying either true or false. You must construct your queries with syntax supported by the ArcSight Database.

Parameters

You can include the following parameters:
- AND (&&)
- OR (||)
- NOT (|)
- LIKE

How Do I Use This?

- You want to construct filter your search results to display numerical data between 10 and 50.

```
…|wheresql bytesOut between 10 and 50
```

- Match the company name of a device vendor.

```
… | wheresql regexp_ilike(deviceVendor, 'Company_Name')
```

Syntax Recommendations

> ⚠️ In a query statement, the wheresql operator treats everything following the "wheresql" name as string values. It is important that each field in the selected fieldset uses valid names (including spelling and capitalization) that matches what is present in the database. Otherwise, the search generates errors.
>
> To determine the exact spelling and capitalization of each field in your fieldset, click **Manage** and select the fieldset name you are using. You can use this page as a reference when you write your query or to troubleshoot if you receive an error message.

Use the following syntax to ensure searches and schedule searches that use the "wheresql" condition succeed:

- As with all search operators, the operator name must be in all lower case letters.

- Fields must have valid names as listed in the ArcSight Database.

- Enclose **string** values in single quotes. For example, use name = 'TCP' instead of name = TCP. (Fields should be named exactly as in the ArcSight Database when using wheresql. In this case, Name with uppercase would cause an error.)

- If **mathematical operators** such as square root or pi **contain a pipe**, the wheresql condition must be enclosed in double quotes. For example:

  |wheresql "bytesin > (|/ 25.0)"

- The "wheresql" condition cannot contain a limit. For example, the following statement is invalid: | wheresql Name = 'TCP' limit 1000

- Do not use the word "wheresql" for the name of a search, a search criteria, or a search query. The "wheresql" is a reserved word for the name of the search operator only.

- Do not use a semicolon at the end of the condition.

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

eval

The **eval** operator displays events after evaluating the results of a specified function. This can be a mathematical, string, or boolean operation and is evaluated when the query is run. The resulting value is assigned to a field name. Once a new field has been defined by the eval operator, it can be used in the query to further refine the search results.

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

General Syntax for Eval

The **eval** operator displays events after evaluating the result of the specified function. Eval operators use the following syntax formats:

```
| eval newField = expression
```

```
EXPRESSION Evaluation of values(fields) or constants with operators
```

where

- *expression* represents a valid field-based query expression.
- Arithmetic expressions or functions are not supported.

Functions that can be used with the eval operator include:

concat, tonumber, tostring, replace(X,Y,Z), abs(X), case(X,"Y",...), ceil(X), ceiling(X), exp(X), floor(X), if(X,Y,Z), isfalse(X), istrue(X), len(X), ln(X), log(X), lower(X), tolower(X), mod(x,y), rand(), round(X), sqrt(X), substr(X,Y,Z), sum(x,y,z,...), trim(X), ltrim(X), rtrim(X), upper (X)toupper(X), urldecode(X).

Aliases that contain special characters have the following syntax restrictions:

Special Characters	Restrictions	Examples
&, !, - , = , % , <, >, |	Need to be enclosed in single/double quotes when they are reused and the search works as expected.	| rename Name as 'DP-V' | eval test = tostring ("DP-V")
@, #, +, ?, /, ^, [], {}, _ , *, ~	Do not need to be enclosed in single/double quotes when they are reused and the search runs as expected.	| rename Name as 'DP@V' | eval test = tostring (DP@V)

For more information about eval functions, see Understand Eval Functions.

Considerations for Using Eval Functions

Please be aware of the following considerations when using the eval functions:

- You might encounter a search error if you run a query that uses both an "All Fields" fieldset and more than five pipeline operations. To avoid this, either reduce the number of fields in the fieldset or reduce the number of pipeline operators in your query.

- The md5(X) function is not supported in a FIPS environment.

Examples

- Could be a simple constant value: "Hello world", 5.

```
... | eval test0 = 5
```

- Could be a simple field: Name, Destination Hostname from the current selected fieldset.

```
... | eval test1 = Name
```

Pipeline operators, such as eval, can use operator chaining to allow output from one pipe operator to be used as input to a subsequent one.

- Find the longest URLs from the vendor ArcSight.

```
deviceVendor = ArcSight |eval urllength=length(requestUrl) |sort
urllength
```

- There is no limit to using arithmetic and boolean operators along with data (in fields or as constants).

```
... | eval test3 = Agent Severity + 1
```

```
... | eval test4 = Name and Device Vendor
```

```
... | eval test5 = (Name and Device Vendor) / 2
```

If the boolean operator is the last operation applied, the overall result will be {0,1}.

- Examples of expressions that use arithmetic and boolean operators:

```
... | eval test6 = upper(Agent Severity ) + 1
```

```
... | eval test6 = upper(Agent Severity ) and Name
```

If the boolean operator is the last operation applied the overall result will be {0,1}.

- Example using "if" and "case" statements:

```
... | eval test = if ( deviceCustomNumber1 = 200, Success, Failure)
… | eval test = case ( deviceCustomNumber1 = 200, Success,
deviceCustomNumber1 = 400, Failure, Unknown)
```

- "Case" requires a final parameter that serves as the else condition. For example:

```
case(name = 'Mandy', 'analyst', name = 'Oskar', 'operator', unknown')
where 'unknown' is the else condition.
```

- Functions can receive other expressions as input:

```
...  | eval test6 = upper(Agent Severity and 1 ) and Name
```

Restrictions

Some functions have restrictions based on the data type:

The following expression is not allowed because two different data types (Name and 1) are not allowed in an arithmetic operation.

```
... | eval test1 = Name + 1
```

The expression below is not allowed because **replace** expects string data types for parameters.

```
... | eval test1 = Name and replace ( 1 , Name , Name )
```

For more information about syntax requirements that the query must meet, see Understand the Query Syntax.

Understand Eval Functions

Eval allows you to define and name an expression that is returned in the search. Use the following functions to build an eval expression:

- Comparison and Conditional Functions

- Boolean Functions

- Cryptographic Function

- Informational Function

- [Statistical Functions](#)

- [Text Functions](#)

For more information about other operators, functions, and syntax requirements, see [eval](#).

Comparison and Conditional Functions

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.

- In the list of expressions, all elements must be of same type.

- Parameters are the values used in the test.

- The only supported types are numeric and string. X can be a number, field or expression.

```
... | eval username = coalesce (Source Username, Destination
Username)
Returns: Username
```

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.

- X and Y can be a number, field or expression. Y must have same data type that X.

```
... | eval newField = nullif(2, 3)
Returns: 2
```

```
... | eval newField = nullif(2, 2)
Returns: null
```

Boolean Functions

and (&&), or (||), not (|), and **like**

- Results of boolean expressions are binary, meaning they satisfy conditions that are true/false, etc.

- You can connect and nest keywords. For example, (boolean_check_a) **and** (boolean_check_b).

- Use parentheses to group boolean operations.

- Each parenthesis should only do one binary "and/or" operation.

- Do not use more two boolean operators to connect keyword clauses. Instead, use parentheses to nest clauses. For example:

  Not allowed: (boolean_check_a) **and** (boolean_check_b) **and** (boolean_check_c)

  Allowed: ((boolean_check_a) **and** (boolean_check_b)) **and** (boolean_check_c)

```
| eval test_auto = (Agent Severity equals 4) and (Agent Severity
equals 0)
```

```
| eval test_auto = (( Agent Severity equals 4 ) and ( Agent Severity
equals 0 )) and ( Agent Severity equals 2 )
```

Cryptographic Function

md5(*X*)

- Calculates the MD5 hash of string, returning the result as a string in hexadecimal.

- *X* must be a string.

```
... | eval usermd5 = md5 (Destination Username)
Returns: 202cb962ac59075b964b07152d234b70
```

> The md5(X) function is not supported in a FIPS environment.

Informational Function

isnull(*X*)

- Returns true if the *X* is null otherwise returns false.

```
... | eval newField = isnull(2)
Returns: false
```

Statistical Functions

greatest(*X*,*Y*[,*Z*,*N*, ...])

- Returns the largest value in a list of expressions. The list is up to 20 elements long.

- In the list of expressions all elements must be of same type.

- The only supported types are numeric and string. *X* can be a number, field or expression.

```
... | eval newField = greatest(7, 5, 9)
Returns: 9
```

```
... | eval newField = greatest('sit', 'site', 'sight')
Returns: site
```

```
... | eval newField = greatest(bytesIn, 100)
Returns: 100, when bytesIn is less than 100
```

least(*X,Y[,Z,N, ...]*)

- Returns the smallest value in a list of expressions. The list is up to 20 elements long.

- In the list of expressions all elements must be of same type.

- The only supported types are numeric and string. *X* can be a number, field or expression.

```
.. | eval newField = least(bytesIn, bytesOut)
Returns: 5
```

```
... | eval newField = least('sit', 'site', 'sight')
Returns: sight
```

```
... | eval newField = least(bytesIn, 100)
Returns: 100, when bytesIn is greater than 100
```

randomint(*X*)

- Returns a random number between 0 and *X*-1.

- *X* can be any positive integer between the values 1 and 9,223,372,036,854,775,807.

```
... | eval newField = randomint(10)
Returns: a random number between 0 and 9
```

Text Functions

length(*X*)

- Returns the character length of a string, *X*.

```
... | eval n=length(field)
Returns: the length of (field). If the field is 256 characters long,
it returns n=256.
```

```
... | eval n=length("abc")
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" )
... | eval name=tolower("USERNAME" )
Returns: the value of the field username in lowercase. If the
username field contains FRED BROWN, it returns name=fredbrown.
```

substr(*X,Y,Z*)

- This function returns a new string that is a substring of string *X*.

- The substring begins with the character at index *Y* and extends up to the character at index *Z*-1.

- The index is a number that indicates the location of the characters in string *X*, from left to right, starting with zero.

- *Y* can be negative.

- *Z* cannot be negative.

```
...| eval n=substr("ArcSight", 5, 6)
Returns: "g"
```

```
...| eval n=substr("ArcSight", 2, 6)
Returns: "cSig"
```

```
...| eval n=substr("ArcSight", 0, 3)
Returns: "Arc"
```

trim(*X*)

- trim(*X*) removes all spaces from both sides of the string *X*.

ltrim(*X*)

- ltrim(*X*) removes all spaces from the left side of the string *X*.

rtrim(*X*)

- rtrim(*X*) removes all spaces from the right side of the string *X*.

  For the sake of these following examples, assume that *X* is a literal string and _ represents any number of space characters.

```
... | eval trimmed=ltrim("_string_")
Returns: trimmed="string_"
```

```
... | eval trimmed=rtrim("_string_")
Returns: trimmed="_string"
```

```
... | eval trimmed=trim("_string_")
Returns: "string"
```

upper(X)

- Takes one string argument and returns the uppercase version.

```
... | eval name=upper("username")
... | eval name=toupper("username")
Returns: the value of the field username in uppercase. If username
contains fred brown, it returns name=FRED BROWN.
```

For more information about syntax requirements that the query must meet, see
Understand the Query Syntax.

concat

The **concat** function creates a new string field that concatenates (or links together) strings
from fields. It concatenates any user-defined strings that are separated by a comma (",").

Search converts IP and MAC binary fields into a more user-friendly string format and then
concatenated. Date fields are converted to the user format that is configured in your user
preferences. Search converts NULL values to empty string fields. The maximum limit for
concat results is 6,000 characters. Anything longer than this will be truncated.

- Syntax

- Parameters

- How Do I Use This?

Syntax

Syntax for concat should look like this:

```
... | eval newField = concat([field|value]*)
```

where:

- *newField* represents the field that you want to evaluate or test.

- *field* represents a string field in the result.

Parameters

The concat function can receive from 1 to 20 parameters, which can be expressions, user
defined strings, or fields from the fieldset.

```
| eval test0 = concat('Event Name: ',  'Name')
```

```
| eval test1 = concat ( 'Event Name: ' , upper ( Name ) )
```

```
| eval test0 = concat ( 'Event Name: ' , ceil ( 2 ) )
```

```
| eval test0 = concat ( 'Event Name: ' , ceil ( 2 ) , replace ( Name ,
'HTTP' , 'MQTT' ) )
```

How Do I Use This?

- Create an eval search that concatenates fields related to a Host:

```
| eval Host = concat(destinationHostName, ':' ,destinationPort)  -
sample output - mf.com:9000
```

- Create an eval search that concatenates fields related to the identity of an employee:

```
| eval Employee = concat(FirstName,' - ', LastName,  ' - ',
DeptName,'(', srcUserName, ')')
```

For information about other operators, functions, and syntax requirements, see Use an
Operator in the Query.

if and case

If() and **case()** are both eval operators that expect specified conditions be met (are True). An
if statement returns a value when the given condition is met (is True), or returns another
value when the given condition is not met (is False). A **case expression** runs through a set of
given conditions and returns a value when the first condition is met (is True). Once the
condition is met, the application stops any further searching for that condition. If no
conditions are met (is False), then the software returns NULL.

When if() and case() are used together and the case expression is met (is True), the if
statement returns that condition's values accordingly. If the case expression is not met (is
False), then the application searches for the next condition given for the case expression.

- Syntax
- How Do I Use This?

Syntax

if

```
| eval test = if ( deviceCustomNumber1 = 200, Success, Failure)
```

case

```
| eval test = case ( deviceCustomNumber1 = 200, Success,
deviceCustomNumber1 = 400, Failure, Unknown)
```

The operators support conditional expressions, such as >, >=, <, <=, =, etc.

How Do I Use This?

Less than

if

- I want to determine if incoming bytes are less than 5000 and to identify the lowest and highest values of incoming bytes.

```
bytes in != null | eval test = if ( bytes in < 5000 , Low , High )
```

case

- I want to identify instances where incoming or outgoing bytes are below 3000 and return the lowest and highest values for each category.

```
bytes in != null AND bytes out is not null | eval test = case ( bytes
in < 3000 , Low , Bytes out < 3000, Low, High )
```

Equals

if

- I want to know all instances with an agent severity of 3.

```
agent severity != null | eval test = if ( agent severity = 3 ,
Success , Failure )
```

case

- Show me the device with the identification number 170011; otherwise show me the device with the identification number 3.

```
deviceCustomNumber1 is not null | eval test = case (
deviceCustomNumber1 = 170011 , Success , deviceCustomNumber1 = 3 ,
Failure , Unknown )
```

Contains numbers

if

- I want to identify all instances with a severity rating of zero (0) or one (1).

```
agent severity is not null  | eval test = if ( agent severity = 1 , 1
, 0 )
```

case

- Show me which devices have encountered a severity level of four (4); otherwise show me the highest and lowest severity levels.

```
agent severity is not null AND priority is not null | eval test =
case ( agent severity = 4 , SHigh , priority > 5 , PHigh , other )
```

Three conditions

case

- I want to test three conditions (username, category outcome, and category technique) to identify Arcsight user names, any failed category outcomes, and any category techniques that might be exploited or represent vulnerabilities.

```
source username != null AND category outcome != null AND category
technique is not null | eval test = case ( source username = Arcsight
, Arcsight , category outcome = '/Failure' , Failure , Category
Technique = '/Exploit/Vulnerability' , Vulnerability , other )
```

For information about other operators, functions, and syntax requirements, see General Syntax for Eval, Understand Eval Functions, and Use an Operator in the Query.

replace

The **replace** is a function of the eval operator that provides a mechanism to replace the content (expressed as string) of a field and to return the value in a new field. Before using replace, create a query that contains string values in its fields. When using replace, the process transforms the data into temporary tables so that the transformation occurs after the main query is executed.

- Syntax
- Parameters
- How Do I Use This?

Syntax

```
Name is not null | eval test = replace(Name, "Response", "Returned Value")
```

where

- Name, Response, and Returned Value are the parameters used in the replacement function

- The replace function is case sensitive. For example, "This," "THIS," and "this" are considered three different words. Match the exact string in order to replace it

Parameters

Replace has three parameters:

- **Name**, the source string value

- **Response**, the match value that will be substituted with the returned value in the results

- **Returned Value**, the replacement value

How Do I Use This?

Use replace when you want to obfuscate data, improve the context of a field, or make reading the text more intuitive.

You can also use the replace function to replace an entire string.

- In this example, use replace to substitute a device's vendor name with OpenText.

```
| eval newDeviceVendor = replace ( deviceVendor, "HPE", "OpenText")
```

where:

- `DeviceVendor` is the source name for the string value.

- `HPE` is the response value.

- `OpenText` is the returned value.

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

tonumber

The **tonumber** eval function converts string fields into floating point numbers so that the data can be applied to additional calculations. If a result cannot be expressed as a number, Search leaves the field empty.

- Syntax
- Parameters
- How Do I Use This?

Syntax

```
suboperator : tonumber
```

```
search_criteria | eval alias_name = tonumber one_field)
```

where:

- *search_criteria* represents a non-pipe operator query statement, such as "deviceVendor IS NOT NULL."
- *alias_name* represents a valid field alias.
- *one_field* represents a valid field as a parameter for "tonumber."

Parameters

There can be only one *fieldName* such as a device vendor or a version.

How Do I Use This?

Use tonumber to convert string values to numbers.

- Create a search query that converts log messages to numbers:

```
| eval messagesAsNumber = tonumber ( message )
```

- Create a search query that converts vendor devices to numbers:

```
| eval x = tonumber ( deviceVendor )
```

- Create a search query that checks for vendor device data that is not NULL and convert the data from version fields to numbers:

```
deviceVendor IS NOT NULL | eval test = abs ( 10 ) + 10 | eval
toNumberAlias = tonumber(version) | eval test2 = abs (13)
```

- Filter the data for those entries where ArcSight is the device vendor. Transform the version to a number and the device's custom number to a string value:

```
Device Vendor = "ArcSight" | eval toNumberAlias = tonumber(version) |
eval numberToString = tostring (deviceCustomNumber1)
```

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

tostring

The **tostring** function is used in an eval operation to convert fields into string values. The input for tostring can be string values, numbers, integers, double point, float, IP/MAC address, and dates. All of these inputs must come from a field in the ArcSight Database.

- Syntax

- Parameters

- How Do I Use This?

Syntax

```
search_criteria [pipe_operator]* eval alias_name = tostring (one_field)
[pipe_operator]*]*
```

where:

- *search_criteria* represents the criteria being tested in the query.

- *pipe_operator* represents the pipe operation for the query.

- *alias_name* represents the field to be converted to a string value.

Parameters

The function only accepts one parameter. More than that will cause an error. The parameter can be a field that represents a string, number, IP address, MAC address, and date. If the parameter is null, it returns a null input.

How Do I Use This?

Here are examples of queries using tostring:

```
... | eval testString = tostring(Name)
```

```
Name not equal null | eval testNumber = tostring(AgentSeverity)
```

```
... | eval testmac = tostring(Agent Mac Address)
```

```
... | eval testData = tostring(Device Receipt Time)
```

```
Agent Address not equal null | eval testIp = tostring(Agent Address)
```

For information about other operators, functions, and syntax requirements, see Use an Operator in the Query.

Understand the Search Criteria

The **search criteria** defines the settings for your search, the time range in which to find data and the fieldsets that you want to use for displaying the results. Search provides system searches that you can view and load, such as DoS Events, MITRE ATT&CK Events, and Failed Login Event.

You must have the required permissions for saving search criteria. For example, you must have the **Manage Search Criteria** permission to save criteria such as fieldsets. You can also save your search criteria for future use, such as loading the criteria into another search. You have the option to clone, modify, or remove a saved criteria at any time.

Manage the Fields Displayed in Search Results

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

- **System Fieldsets**: Predefined fieldsets provided by the system.

- **My Fieldsets**: Customize the default fieldsets and lookup list fields for individual purposes.

New searches display the user´s default fieldset. These will remain selected in the fieldsets list box even when moving to other search tabs. If you select another fieldset, the pop-up window closes to display the new option. You can revert the change to the previously selected fieldset.

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

Create a Fieldset

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

1. From the **Search** page, click the icon to the left of the search name.

2. From the selected search's tab, click the menu and select a fieldset from the list in the **My Fieldsets**panel.

3. Click **Manage**.

4. Click **+** to add a new fieldset.

5. Enter a **Fieldset Name**.

   - Each fieldset should have a unique name.

   - Fieldset names are not case sensitive.

   - The fieldset is used only for your search results and does not affect other users connecting to the same system.

   - Creating a fieldset that does not contain any fields causes an error in the application.

6. Select a **Category** and drag and drop any of the **Fields** to the to the **Selected Fields** column.

7. Click **Save**.

8. (Optional) Select **Apply to This Search** to customize the original fieldset without overwriting or saving it.

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

Edit a Fieldset

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

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

   - Editing the Selected Fieldset

   - Editing a Different Fieldset

   - Cloning a Fieldset

Editing the Selected Fieldset

1. From the **Search** page, click the icon to the left of the fieldset name.

2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.

3. From the fieldsets window, select **Edit**.

The **Edit Fieldset** window displays.

4. Drag and drop any field to the **Selected Fields** column OR select **Text Editor** to write the fields you need.

5. To locate a specific field, use the **Search** field.

6. In the **Fieldset Name** field, update the fieldset name as needed. The fieldset is used only for your search results and does not affect other users connecting to the same system.

7. Click **Save**.

8. (Optional) Select **Apply to This Search** to customize the existing fieldset without overwriting or saving it.

   The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporary custom fieldset at a time.

Editing a Different Fieldset

1. From the **Search** page, click the icon to the left of the fieldset name.

2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.

3. Click **Manage**.

4. Select the fieldset checkbox.

5. Click the **Edit fieldset(s)** icon.

   The Edit Fieldset window displays.

6. Drag and drop any field to the **Selected Fields** column OR select **Text Editor** to write the fields you need.

7. To locate a specific field, use the **Search** field.

8. In the **Fieldset Name** field, update the fieldset name as needed. The fieldset is used only for your search results and does not affect other users connecting to the same system.

9. Click **Save**.

10. (Optional) Select **Apply to This Search** to customize the existing fieldset without overwriting or saving it.

    The temporary fieldset will not be visible to other users, and it will only remain available on that session. After you log out, the system removes the temporary fieldset. You can have one temporary custom fieldset at a time.

Cloning a Fieldset

You can make a copy of a fieldset you have created. Edit this copy to save you from creating a completely new fieldset.

1. From the **Search** page, click the icon to the left of the fieldset name.

2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.

3. Click **Manage**.

4. Select the fieldset checkbox.

5. Click the **Clone fieldset(s)** icon to make a copy of the selected fieldset.

Delete a Fieldset

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

You can delete a fieldset that you have created. If you delete a fieldset that's used in an active search, Search changes the fieldset name to **Custom** for that search. If you delete a fieldset used in a saved search query or saved search criteria, Search will use the default fieldset saved in your user preferences. You cannot delete a system fieldset.

1. From the **Search** page, click the icon to the left of the fieldset name.

2. From the fieldsets window, click the fieldset menu and select a fieldset from the list in the My Fieldsets panel.

3. Click **Manage**.

4. Select the fieldset checkbox.

5. Click the **Remove fieldset(s)** icon.

6. Click **Yes** to proceed.

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, Search updates data upon re-executing the search based on the most recent 30 minutes. Alternatively, you can create a dynamic date range.

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

- Specify a Dynamic Date Range
- Understand the Search Timestamps for Events
- Understand How Time Zones Affect Search Results

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:

When viewing a search or starting a query, select the currently specified time range.

For the start or end time under **Custom Range**, select **Dynamic**.

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

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

Value	Represents
m (lowercase)	Minutes
h	Hours

Value	Represents
d	Days
w	Weeks
M (uppercase)	Months

Understand the Search Timestamps 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 when searching for events.

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 (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 (NET)

Represents the best known time for an event. Ideally NET is the time when the connected device reported that the event occurred (the DRT) because the device is the most direct known observer of the event occurrence. However, when the DRT for an event is not within a credible time range compared to the database's time, NET represents the time when the database received the event (the dBRT). For example, the time on a connected device was configured incorrectly such that DRT for an event is May 29 1975 when the current date in the database when the database received the event is June 29 2020. The database recognizes that the event's May 29 1975 timestamp for DRT is outside the credible time range. Based on the discrepancy with DRT, the database sets NET to June 29 2020 (same as the dBRT).

By default, the DRT value must be within a boundary of -7 days in the past and +1 days in the future from the dBRT. To configure the boundary criteria in a non-SaaS environment, see the *Administrator's Guide to ArcSight Platform 23.3*.

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 Histogram 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 Histogram has seven bars in the original time zone, the number of bars could increase or decrease to reflect the currently specified time zone.

Extend the Search with a Lookup List

Select **Configuration** > **Lookup Lists**.

You can make **lookup lists** from CSV files that contain common fields that you might want to include in your searches. The system stores the data in the CSV file in a database table, which then becomes available for use in a search. You can add fields from a lookup list to fieldsets and use them in search queries.

- Understand the Considerations for the Lookup List File

- Create a Lookup List

- Append a Lookup List

- Replace a Lookup List

- Delete a Lookup List

Understand the 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.

- For search operations, the corresponding data types for lookup lists with variable characters (or varchars) are short text (VarShort) and long text (VarLong).

- The remaining rows must be comma-separated values for the fields in the first row.

- Do not include spaces before, after, or within a field name.

- 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. Click **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	The name of the lookup list
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

Value type	Specifies
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, click **Upload**.

Append a Lookup List

Use the **Append** feature to add more rows to a current lookup list.

- The file you need to append needs to have the same structure as the one you uploaded. For example, the same amount of columns.

- The file you need to append should not have an empty value in any of its rows.

1. Select **Configuration** > **Lookup Lists**.

2. Click the **eye** icon on the left side of the selected lookup list.

3. Click **Append**.

4. Select the list you want to append.

5. Click **Upload**. The original lookup list will be updated with the new rows added.

Replace a Lookup List

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

1. Select **Configuration** > **Lookup Lists**.

2. Select the list you want to replace.

3. Click the **eye** icon on the left side of the selected lookup list.

4. Click **Replace**.

5. Select the CSV file you want to use to replace the contents of the existing lookup list.

Delete a Lookup List

1. Select **Configuration** > **Lookup Lists**.

2. Select the list you want to delete.

3. Select the **trash can** icon.

Understand System Search Queries and Search Criteria

Search includes the following **out-of-the-box** system search queries and search criteria. All of these system searches are set in Normalized Event Time. For more information about how to use these queries and criteria, see Load a Saved Search.

> **Note:** You can also search queries by using # and the query name. For example, #Configuration changes or #DGA Events. Additionally, you can run criteria searches as queries using the same method. Additionally, there is a list of reserved words that must be enclosed in quotes (" ") to ensure the system correctly parses the query.

Category	Name	Use as	Description
Application Monitoring	Windows New Service Created	Query	Lists events indicating new windows services were created from the following event sources: • Microsoft-Windows-Security-Auditing:4697 • Service Control Manager: 7045
Configuration Monitoring	Configuration changes	Query	Lists configuration changes based on ArcSight categorization.
Entity Monitoring	Failed logins	Query	Lists events indicating failed login activity based on ArcSight categorization.
	Failed Login Events	Criteria	Lists failed login activity events based on ArcSight categorization for the last 30 minutes by default.
	Failed logins for $username	Query	Lists events indicating failed login activity based on ArcSight categorization for a specific user. The user should be specified before running the search.
	Windows account creation	Query	Lists events indicating new windows accounts created based on the following event sources: • Microsoft-Windows-Security-Auditing:4720 • Security:624
Event Monitoring	ESM Correlation Events	Query	Lists ESM correlation events.
Malware Monitoring	Malicious code activity	Query	Lists events indicating malicious code activity based on ArcSight categorization.

Category	Name	Use as	Description
MITRE Monitoring	MITRE ATT&CK Events	Criteria	Lists correlation events reported from Arcsight ESM content package: https://marketplace.microfocus.com/cyberres/content/esm-default-content. These events are forwarded to the ArcSight Database using ArcSight Forwarding connector, or any other flex connector which reports this information, using the following mapping: deviceCustomString6Label='MITRE ID' Where deviceCustomString6 contains the actual MITRE ATT&CK technique.
Network Monitoring	DGA Events	Criteria	Lists DGA-related events based on Microsoft Trace Log.
	DNS Events	Query	Lists DNS-related events.
	DoS Events	Criteria	Lists events indicating denial of service based on ArcSight categorization.
	Firewall drop	Query	Lists Drop Firewall events based on Arcsight categorization for a specific IP address. The IP address should be provided at runtime.
	Firewall drop for $ip		Lists Drop Firewall events based on Arcsight categorization.
	Firewall Events	Criteria	Lists Firewall events based on ArcSight categorization.
	Proxy Events	Criteria	Lists Proxy events based on ArcSight categorization.
	SSH authentication	Query	Lists events indicating SSH Authentication events based on ArcSight categorization.
	VPN connections	Query	Lists events indicating VPN connections based on ArcSight Categorization.
Vulnerability Monitoring	Vulnerabilities Events	Query	Lists events indicating vulnerabilities based on ArcSight categorization and Vulnerability Scanner events.

Creating and Saving Searches

To execute a search, you must enter the query input, a fieldset that you want for the search results, 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 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 configure your preferred default setting. For example, you can configure a default time range. To use the same search query or search criteria for multiple searches, you should **save** it. You can also save the results of an executed search and configure a default expiration time for searches. By default, session searches expire after 24 hours of inactivity and saved searches after seven days. Search truncates long queries, displaying **…** to indicate additional content. To see the entire query, you can **pin** the input field.

Create a Search

Select **Search** > **+**.

When creating a search, you can use the default values for the fieldset, time range of data to search, and some additional settings or specify your preferred settings. Alternatively, you can load a saved query, criteria, or dataset.

If you tend to use the same settings for some search parameters, you might want to configure your preferred default setting. For example, you can configure a default time range. To use the same search query or search criteria for multiple searches, you should **save** it. You can also save the results of an executed search and configure a default expiration time for searches. By default, session searches expire after 24 hours of inactivity and saved searches after seven days. Search truncates long queries, displaying **…** to indicate additional content. To see the entire query, you can **pin** the input field.

If you do not have Real-time Threat Detection Service in your ArcSight SaaS environment, then you can create only one type of search in UI which corresponds to fixed-time search.

Create a Fixed-time Search

A fixed-time search uses a custom range with specific start and end dates. You can choose to specify dynamic dates, such as midnight on the first day of the current month.

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

2. Enter the query in one of following ways:

   - To use a predefined System search, type **#**.

     The predefined searches might provide only a query expression or include search criteria such as a specific time range.

- To use a search operator, such as eval and wheresql, begin typing the operator's syntax.

  For example, type:

  `... | where <expression>`

- To manually enter the query, begin typing the expression.

  For example, type :

  `Source Address = 192.10.11.12 and Destination Address= 192.10.11.12 or Destination Address in Subnet 192.10.*.*`

- To use a saved query, criteria, or search results, select 📁.

- To search data migrated from ArcSight Logger, select **Logger** from the list box next to the **Search** button.

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

> In the query, Search treats a comma (,) between the search fields and values as an OR operator.

3. (Optional) To view all content in a very large query, select the **Pin** icon in the query input field.

   Otherwise, Search truncates long queries, displaying … to indicate additional content.

4. Specify the fieldset that you want for displaying the search results.

   By default, Search displays your preferred default fieldset. If you have not specified one, Search displays the *Base Event Fields* fieldset.

5. Click **Fixed-time**. (For a SaaS environment, if you do not have the Real-time Threat Detection Service, the application automatically defaults to Fixed-time.)

6. For the time range, perform **one** of the following actions:

   - From the menu, select a pre-defined value under **Quick Ranges**.

   - From the menu, use the **Custom Range** fields to specify a time range.

   - From the menu, select **Dynamic**, and 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 (NET) by default.

7. (Optional) To limit the number of results received from the search, complete the following steps:

a. Select ⚙ to the right of the query input field.

b. For **Maximum search results**, specify the maximum number of results that you want to receive in the dataset.

8. (Optional) If you do not want this search to expire in the default time, complete the following steps:

a. Select ⚙ to the right of the query input field.

b. For **Search expires in**, specify the number of hours that Search will store the session.

9. (Optional) To more easily find this session search later, give the search a name.

10. (Optional) To run the search, click **Search**.

Alternatively, you can press **Enter** when editing the query input field.

11. (Optional) To save the query, criteria, or search results for future use, select the **Save** icon.

For additional information about viewing results and saving fixed time searches, see View the Event Inspector and Save a Fixed-time Search. For information about fixed-time search limits, see Limits for Fixed-time Searches. For information about real-time searches, see Understand Fixed-time versus Real-time Searches.

Create a Real-time Search

Requires the Real-time Threat Detection service in the ArcSight SaaS environment.

Real-time searches show live results of your query, based on a start time that you specify (for example, the last 30 minutes). As long as there is data to satisfy the query, the Results Table and Event Histogram continue to build, and the time scale below the histogram continues to show progress.

> Real-time search is not available for data imported from Logger.

1. Display the **Search** tab.

2. Enter a query in the search field.

3. Define the search settings.

4. Click the drop-down menu for the **Timestamp** interval.

5. Select the type of **Timestamp** for the event.

Search uses Normalized Event Time (NET) by default.

6. Click **Real-time**.

    The user interface displays only settings related to real-time searches. As your search results are returned, the screen, including the event histogram, refreshes every 30 seconds.

7. Select a **Start time from**. Your choices are **Last 5 Minutes**, **Last 15 Minutes**, **Last 30 Minutes**, **Last 1 Hour**, and **Last 12 Hours**.

8. (Optional) Check or uncheck the "Do not accumulate data" option, based on how you want the default histogram start time behavior to be.

    Data will be accumulated in the background, this option pertains only to the default histogram time window behavior. For more information about real-time search limits, see Understand Search Start Times and Limits for Real-time Searches.

9. Click **Search**.

> Even if it is not selected in the current fieldset, Database Receipt Time field is automatically displayed for real-time searches.

You can run at most 25 concurrent real-time searches.

For information about viewing the results of and saving real-time searches, see View the Results of a Real-time Search and Save a Real-time Search.

For information about creating a fixed-time search, see Create a Fixed-time Search.

Save a Search

You have the ability to save searches that you want to run or review often. You can save the search query; the query plus the criteria for the search; or the results of the search, which includes the query and criteria.

Save a Fixed-time Search

In a Search tab, select **Save**.

You can save a fixed-time search, including its query and criteria, to rerun at your convenience. To save just the query or the query and criteria, you do not need to execute the search.

1. In the Search tab, select the **Save** icon.

2. Select which part of the search you want to save:

   - Search Query

   - Search Criteria

   - Search Results (Dataset)

3. Specify a name for the saved search.

   - Each saved search must have a unique name.

   - We do not recommend using the same names for saved search queries, criteria, and results.

4. (Conditional) When saving the search results, specify how long you want to store the dataset.

   For example, if you have the *Never Expire Search Results* permission, you can configure the search results to never expire.

5. Select **Save**.

For information about creating and viewing results of fixed-time searches, see Create a Fixed-time Search and View the Event Inspector .

Save a Real-time Search

Requires the Real-time Threat Detection service in the ArcSight SaaS environment.

You can save the results of your real-time search. The saved dataset can include all received events or just the events associated with the current histogram range. You must pause the search to save the current dataset. However, the system continues to receive events for the search in the background. Thus the number of saved events might be slightly greater than events in the Results Table at the moment you paused the search.

1. In the **Search** tab, pause the search.

2. Click the **Save** icon 💾.

3. Select **Search Results (Dataset)**.

   You also can choose to save just the search criteria.

4. Specify a name for the saved search.

- Each saved search must have a unique name.

- We do not recommend using the same names for saved search queries, criteria, and results.

5. Specify the time range of the events that you want to save:

Histogram time range
> Saves only the events associated with the time range currently displayed in the Event Histogram. For example, 7:30 AM to 9:12 AM.

Entire time range
> Saves all results received for the search.

6. Specify how long you want to store the dataset.

   For example, if you have Log Management and Compliance (Recon) and the *Never Expire Search Results* permission, you can configure the search results to never expire. By default, saved results expire after 7 days or your preferred setting.

7. Select **Save**.

For more information about creating and viewing the results of a real-time search, see Create a Real-time Search and View the Results of a Real-time Search.

Load a Saved Search

If you have saved a query, criteria, or search results, you can load that saved item in a Search tab. You can also load the predefined search queries and criteria.

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

2. Select 📁 above the query input field.

3. Select the tab relevant to the saved search that you want to load:

   - Search Query

   - Search Criteria

   - Search Results

4. Select the saved search that you want to load.

5. Select **Load**.

6. (Optional) Modify the search settings as needed, then run the search.

7. (Optional) To more easily find this session search later, give the search a name.

8. (Optional) To save your changes as a new search, select 💾.

Run a Search

When you run a search, Search begins populating the Events histogram 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.

1. Create or load the search that you want to run.

2. Click **Search**.

3. (Optional) To more easily find this search later, give the search a name.

4. (Optional) To save the query, criteria, or search results for future use, select the **Save** icon.

5. Click the **pause** or **stop** icons if you need to interrupt the search. Click the **resume** icon to continue the search.

Modify the Search Query or Criteria

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

1. In the Search tab, 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**.

Name a Search

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

1. Right-click the name of the tab.

2. Select **Rename**.

3. Type the custom name.

4. Press **Enter**.

5. (Optional) To save the search, click the **Save** icon.

Search Event Data from Logger

You can search Logger archived events using the same parameters as in regular searches.

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

- The query uses only the specific set of operators available in the Search feature. If you are used to the query format in Logger, we recommend that you review the query functionality in Search.

- Your searches can include data from Logger storage groups even if the Logger storage groups do not display as part of the ArcSight Database's configuration.

- Before searching for Logger events from a particular Logger, metadata from that Logger must have already been imported, and at least one data migration from that Logger must have been completed.

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

2. From the list box next to the **Search** button, select **Logger**.

3. Add the required query details.

   You must use the search operators supported in ArcSight Platform.

4. Click **Search**.

> Note: If UTC time wasn't specified in the time range for importing events, you will need to convert the archive UTC timestamp shown in the **Import Logger Data** tab to your browser time/selected time zone, and enter that value as search time to fetch events from that time range.

Use a URL to Create, Update, and Navigate Searches

Search lets you create, navigate, and update searches by modifying a URL. This is a quick way to integrate with other applications or to simply save your current search for future use.

Creating Searches

Open Search and create a new search with default values:

```
/rec/search
```

Create a new search with given criteria.

```
/rec/search?query=Name+not+equals+null&fieldsetId=3223931b-b439-4951-a2d2-
d83f9506c109&startDate=1673567387483&endDate=1673569187483
```

Opening Searches

Open a specific search by the ID. The app will automatically add criteria to the URL after opening the search.

```
/rec/search/:searchId
```

```
/rec/search/home
```

Updating Searches

Open a specific search by the ID and update the values. The app will ask you if your choice is the desired behavior.

```
/rec/search/:searchId?query=Name+not+equals+null
```

Opening a Search in the Event Inspector

Open a specific event by GEID, ID, and Event Table in the Event Inspector tab:

```
/rec/search/eventsInspector?eventsDetail=
[{"geid":":globalEventId","id"::Id,"eventsTable":":table"}]
```

> Sometimes, the timestamp for the DBRT (Database Receipt Time) is not selected correctly, as in the case for the URL
> <FQDN>/re/search?query=Name%20<>%20null&timeColumn=persistedTime . This happens when you navigate to the URL from some (but not all) features in the system. Additionally, if you are not signed in and try to navigate to this URL, the search is not created, and the timestamp is not selected.

Viewing and Managing Your Searches

The dataset for your **search results** reflect events that match the search query and criteria settings that you specify. Search displays the results in an Events Histogram, Results Table, and Event Inspector. You can save the queries, parameter sets, and results datasets for future use.

If the connectors are configured to send raw events, the table and inspector panel can include raw event data. Also, the maximum number of events that a search can return is 10 million, but you can specify a preferred **search results limit**. If your searches regularly stop at the maximum limit, consider splitting the query into separate searches. Alternatively, you can refine the results by adding an operator such as *where* to the query.

You can export the search results to a .csv file or export a single result to a .pdf file.

Get an Overview of Your Searches

Select **Search** > **Home**.

The **Search Home** tab provides a high-level view of your Search and event activity while also offering immediate access to search features. Your Search and event activity are segmented into Widgets that show the state of specific searches and events, such as saved search queries, search criteria, and events by agent type. To view the items referenced in a search chart, such as saved search queries, click ⬚.

> The data in the events pie charts (Total Events, Total Events - 24 Hours, Events by Device Vendor - 24 Hours, etc.) refreshes every five minutes and is based on a normalized event time.

My Session Searches

> Lists all recent searches. For each search, the table provides the name, search query, status, search type, timestamp, fieldsets, the ID that created the search, and the date the search was created. You can sort the table by some of the column. The table show only searches with the status Completed, Pause, Running, and Error.
>
> To view one of the searches, click 🔍. To remove session searches from the list, select the rows to be removed. Then, click 🗑.

Search Queries

> Shows the number of system, private, and public saved search queries that you can access.

Search Criteria

> Shows the number of system, private, and public saved search criteria that you can access.

Search Results

> Indicates whether any of your saved search results have completed, are running, or have been paused.

Fieldsets

> Shows the number of system and private fieldsets that you can use when running a search.

Lists

> Shows the number of lookup lists that you can include in a search.

Total Events

> Shows the total number of all events that have occurred within your ArcSight database installation. This number refreshes every five minutes.

Events 24 Hours

> Shows the total number of all events within the last 24 hours.

Events by Device Vendor - 24 Hours

Shows the total number of the first three events by device vendor with the highest count within the last 24 hours.

Events by Agent Type - 24 Hours
Shows the total number of the first three events by agent type with the highest count within the last 24 hours.

Events by Agent Severity – 24 hours
Shows the total number of the first three events by agent severity with the highest count within the last 24 hours.

View the Events Histogram

The **Events Histogram** displays data in a segmented graph where the y-axis presents the number of events per bars of time segments in the x-axis. The time range on the x-axis might not match the time range specified in the search query because the start and end times on the x-axis are determined by the event times of the first and last matching events of the search query.

Click the menu to the right of the histogram and select either **Linear Scale** or **Log Scale** to display the data in your preferred format.Click the **Settings** icon (⚙) and select either **Linear Scale** or **Log Scale** to display the data in your preferred format. You may also select **Hide Histogram** if you do not wish to display the histogram. As you hover your pointer over the histogram, the bar color directly below the pointer changes and displays a tooltip of the day/date/time of that event range. Click a bar to view event information for a specific time range. Click again to deselect the bar.

Note that some search activities do not require the histogram, and thus it will not be displayed. For example, if you perform an aggregation operation, such as "top" or "bottom," Search will not display the histogram because the Search Results table contains the aggregation of results, not events in a timeline.

How Search builds the histogram

Search progressively builds the histogram as it receives events that match the search settings. If the search needs to scan a large amount of data or a large time period, the histogram displayed initially might refresh multiple times while the search is running. To view the complete histogram of a search, wait until the search has finished running.

Search plots the first one million matching events on the histogram. If a search results exceed one million events, Search displays an informational message. If you need to use the histogram view for event analysis of a search that matches more than one million events, we suggest that you adjust the time range to retrieve fewer than one million events. This will allow you to obtain a complete and meaningful histogram. You can also

use a pipeline operator to further refine search results so that the total number of hits is under one million events.

Narrow the scope of the search

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, adjust the boundaries of the displayed bars. As you adjust the time range within the Histogram, the Events table displays corresponding events.

Drill down to events

You can drill down to events in a specific time period by clicking the bar on the histogram that represents that time period. The bar you drilled down to is highlighted and the events matching that time period are listed below the histogram. To deselect the time period, click the bar again. When you **hover over a histogram bar**, the matching events listed below the histogram do not change, and the histogram continues to display all matching events.

If you are performing a real-time search, zooming or clicking in the histogram automatically pauses a real-time search. For additional information about how a real-time search affects histogram behavior, see Create a Real-time Search.

View the Results Table

The search **Results Table** contains all the fields specified in the fieldset. The dataset contains events associated with the search query and criteria. You can choose to display the table in **Grid View** or **Raw View**. You can perform the following actions while viewing the table:

View all details for an event

To view details of a specific event, right-click the event and select **Open In Event Inspector**. This action opens the Event Inspector in a panel on the right where you can view additional details on the event.

View raw event data

When you click the **Raw View** icon, the Search Results table replaces the fieldset with a Raw Data column, which displays the whole raw 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.

Export all of the search results

You can export all of the results to a .csv by clicking the ⬐ icon.

Export a single event

You can export a single event as a .csv or a .pdf by right-clicking the event and selecting either **Export to PDF** or **Export to CSV**.

Copy a value from an event

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

Compare data in columns

Hover over a column heading, then click the **Pin** icon to pin or unpin a 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.

Reorder columns

To rearrange the order of the columns, drag each column to new position by clicking and dragging the column header.

Sort the data in columns

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

View the Results of a Real-time Search

As with a fixed-time search, a real-time search results displays events that satisfy the query and criteria in the Search Results Table, Events Histogram, and Event Inspector. However, some aspects about pausing and manipulating the display are specific to real-time searches.

1. When you **pause** a real-time search, the interface freezes, but events continue to build in the background as long as there is data to satisfy the search.

   - Clicking the **Pause** ⏸ icon temporarily suspends the search.

   - Automatically pause a real-time search by clicking 🔍⊕ to zoom in.

     Drag the cursor over histogram bars to examine an area of interest. Zooming in automatically freezes the histogram and the search table results. Other ways to automatically pause a real-time search are to click a histogram bar or to scroll in the results table.

   - Observe specific details of the histogram by clicking 🔍⊕ and 🔍⊖ to zoom in and out and click 🔀 to pan across multiple bars in the histogram. The real-time

search will continue to be paused while you perform these actions.

- Move forward and backward in the histogram by clicking the **Back** ⟨ and
  Forward ⟩ icons. The increment of backward or forward time is based on the
  current zoom range.

  For example, if you are zoomed in to a range of 40 minutes, clicking the **Back**
  arrow once will move the histogram backward 40 minutes. Similarly, clicking the
  Forward arrow once will move the histogram forward by 40 minutes at that same
  zoom level. As desired, you can pan the histogram up to the earliest start time or
  the latest (or current time.)

2. To reset the histogram and results table to the starting point when you first paused
   the real-time search, click the **Reset** ↻ icon. Note that this does not resume the
   real-time search; the histogram and results table remain paused.

3. To resume the real-time search, click the **Go to Now** ⊘ icon. This search displays the
   current search results in the histogram and results table.

   Another way to resume a real-time search is to click the **Play** ⊙ icon. For more
   information about the search's start time behavior, see Understanding Start Time and
   Go to Now Behavior.

4. Click ⎙ to export real-time search data to a .csv file or a .pdf file. For real-time
   searches, only data within the time range of the current zoom state in the histogram
   will be exported.

For information about creating and saving real-time searches, see Create a Real-time Search
and Save a Real-time Search.

For information about viewing the fixed-time search results, see View the Event Inspector .

View the Event Inspector

The **Event Inspector** displays additional details for any event you select from the Results
Table. This panel allows you to scroll through the specific details of the event and groups
the details by categories such as **Agent** and **Source**. To open the Event Inspector, right-click
any event in the Search Results table. Then, select **Open in Event Inspector** from the pop-up
menu.

> To view events migrated from Logger, select **Logger** before creating a search.

You can perform the following functions with the Event Inspector:

Search for fields and values

To search for fields and values in the details of an event, enter a string in the search box at the top of the Event Inspector. The Event Inspector will filter the fields and values to match your search criteria.

Add fields and values to current or new search

You can add event fields and values in the Event Inspector to your current search query or a new search query.

Hover over a field (for example, `Agent Hostname`) to display a check box next to the field. Then, select the check box to select the field and its value. Then, either click the magnifying glass icon at the top of the Event Inspector or right-click your selected field. Both actions display a pop-up menu with the following options:

- **Create New Search**

  Allows you to create a new search query with the selected event fields and their values.

  For example, if you selected the field `Name` and its value equals `"failed login"`, then it would display as follows in the new search query: `...| where Name = "failed login"`. The new search will open in a new tab on your web browser. If a field is not already present in the fieldset, it will be added to a temporary fieldset.

- **Add to Active Search**

  Adds your selected event fields and their values to the current search query in the search input field.

  For example, if you selected the field `Name` and its value equals `"failed login"`, the field and value would display as follows in the current search query: `<current search query> | where Name = "failed login"`. If a field is not already present in the fieldset, it will be added to a temporary fieldset.

Create a dashboard based on a host or user profile

You can create a dashboard in the **Reports Portal** that lets you view host and user profile information:

- **View Host Profile**

  To view the details of a host, right-click a host name or an IP address.

  For example, right-click a value in the Agent Hostname column. The system launches a dashboard in the Reports Portal for your selection.

- **View User Profile**

  To view the details of a user, right-click a source or destination username. The system launches a dashboard in the Reports Portal for your selection

Copy and share event detail URL

To share event details with another Analyst, click the **Copy URL** icon at the top of the Event Inspector. This action copies the URL to your clipboard so you can share it as needed.

Export event details to .pdf or .csv files

You can export event details from the Event Inspector to store or share information. You have the option to export events in .pdf or .csv format. Additionally, you can include or exclude null fields in the exported file.

Expand/collapse and show/hide data fields

The top of the Event Inspector contains an arrow icon that expands and collapses the event details. There is also an eye icon that can show or hide null fields. If you select to display null fields and export the event details to PDF or CSV, the exported file will contain the null fields.

View and Use the Details of an Event

Right-click an event in the search Results Table > click **Open In Event Inspector**.

The **Event Inspector** opens in a panel that allows you to scroll through the details of an event and groups them by categories such as **Agent** and **Source**. Use this panel when you want to research specific details on an event. 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. You can only open one event in the Event Inspector at a time.

- Search for Event Details
- Copy and Share Event Detail URL
- Export Event Details to PDF or CSV
- Apply Event Details to Current or New Search
- View Null Data Fields
- Expand or Collapse All Data Fields

> To view events migrated from Logger, select **Logger** before creating a search.

Search for Event Details

The top of the Event Inspector contains a search box that allows you to search through the fields in the event details. Use this feature to quickly locate specific details on an event without the need to scroll through the entire Event Inspector.

To search for fields and values in the details of an event, enter a string in the search box at the top of the Event Inspector. The Event Inspector will filter the fields and values to match your search criteria. For example, if you searched the term "device" the panel will display all fields with the name "device" and any fields containing the value "device".

Copy and Share Event Detail URL

You might want to share the selected event's details with an Analyst or use the details in a report or other media. You can export all content in the Event Inspector with or without empty values. The **Event Inspector URL** contains the event's ID (id field in the Search Results table) and global event ID (geid field in the Search Results table). See the table below for an example and variations of the Event Inspector URL format. Use these formats to create the URL.

Click the **Copy URL** icon at the top of the Event Inspector to copy the Event Inspector URL to your clipboard. Then, you can share the URL as needed. When you load the URL, the Event Inspector open in the browser with the event details related to the search. This action is helpful in situations where you need to research an event further or for reporting purposes.

> If the geid is missing in the URL, an error message will display.

Event Inspector URL	Example
Full Event Inspector URL	/rec/search/eventsInspector/?eventsTable=Recon&id=5139791690&geid=3009625190352082178
geid and id only	/rec/search/eventsInspector/?id=5139791690&geid=3009625190352082178
geid only	/rec/search/eventsInspector/?geid=3009625190352082178

Export Event Details to PDF or CSV

There may be situations where you need to use event details for reporting purposes. Or you might need to share the event details with an analyst who does not have access to the Event Inspector. You can do so by exporting the event details to .pdf or .csv files.

Apply Event Details to Current or New Search

You can add event fields and values in the Event Inspector to your current search query or a new search query. This action is helpful in situations where you need to research more data on a specific event.

Hover over a field in the Event Inspector (for example, `Agent Hostname`) to display a check box next to the field. Then, select the check box to select the field and its value. From here, do one of the following actions:

- Right-click the selected event field

- Click the magnifying glass icon at the top of the Event Inspector

Both actions display a pop-up menu with the following options:

- **Create New Search:** Selecting this option allows you to create a new search query with your selected event fields and their values. For example, if you selected the field `Name` and its value equals `"failed login"`, then it would display as follows in the new search query: `...| where Name = "failed login"`. If a field is not already present in the fieldset, it will be added to a temporary fieldset.

- **Add to Active Search:** Selecting this option adds your selected event fields and their values to the current search query in the search input field. For example, if you selected the field `Name` and its value equals `"failed login"`, the field and value would display as follows in the current search query: `<current search query> | where Name = "failed login"`. If a field is not already present in the fieldset, it will be added to a temporary fieldset.

Once you've performed a new search with the selected field and value pairs, the Event Timeline and Search Results table will filter to display data related to your new search.

Create a Dashboard Based on a Host or User Profile

You can create a dashboard in the **Reports Portal** that lets you view host and user profile information.

- **View Host Profile**: To view the details of a host, right-click a host name or an IP address. For example, right-click a value in the Agent Hostname column. The system launches a dashboard in the Reports Portal for your selection.

- **View User Profile**: To view the details of a user, right-click a source or destination username. The system launches a dashboard in the Reports Portal for your selection.

View or Hide Null Data Fields

To show or hide fields with null data, click the eye icon at the top of the Event Inspector. Hiding the null fields filters your view of the event details to show only fields with data. Use this feature if you want to see only fields with data in the event details.

Expand or Collapse All Data Fields

Next to the eye icon at the top of the Event Inspector is an **Expand All/Collapse All** icon. Click this icon to expand the fields in the Event Inspector to show all values related to the fields. Or click it to hide the values related to the fields and display only the field names.

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
Search Results table	Empty cell
Empty field from Enterprise Security Manager (for example, name=')	name = '', NULL
Event Inspector	--- 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.

Export the Search Results

Once you have created search queries and criteria, run searches, and viewed results or event details, you can choose to export information to retain or share with colleagues.

- Export Search Results
- Export Event Details
- Export Scheduled Searches
- Export Search Queries and Search Criteria

Export Search Results

You can export the Search Results table to a .csv file. Search exports the data, based on the specified fieldset for the search. The export process limits the file to one million event records.

1. In the search toolbar above the histogram, select ⬒.

2. In the resulting **Export Options** dialog box, select either:

   - **Current time range** to export the results shown in the current histogram and search results table.

   - **Original start time** to export the results retrieved from the original start time you selected for the search.

3. Click **Export** to export the result for the selected option to a .csv file.

1. In the search toolbar above the histogram, select ⬒.

2. Choose to save the file or open it in a desired location.

Additionally, you can export a single result from the results table by right-clicking the row and selecting .pdf as the file format.

> Saved .csv files of search queries sometimes contain syntax that uses "name= a special character" (such as "name=+" or "name=_"). In Excel, if the file is not opened properly, you might see formatting issues where the fields display as a generic "#NAME".
>
> To avoid this, open the file by selecting **From Text/CSV** on the Excel **Data** ribbon. Navigate to the .csv file you downloaded and click **Import**. Preview the file to ensure the fields display correctly, then click **Load** to view the full file.

Export Event Details

There may be situations where you need to use event details for reporting purposes. Or you might need to share the event details with an analyst who does not have access to the Event Inspector. You can do so by exporting the event details to .pdf or .csv.

1. At the top of the Event Inspector, click the **Export** icon.

2. Click **Export to PDF** or **Export to CSV**.

   The system starts a download of the event details to your selected format.

3. Share or use the .pdf or .csv as needed.

If you select to show null values, the system includes null values in the exported .csv or .pdf file.

You can also export a single event to a .pdf or .csv file from the **Search Results Table**. Right-click an event in the Search Results table to open a pop-up menu with the options **Export to PDF** and **Export to CSV**. If you use this method to export the event details, null values will be included in the exported file.

Export Scheduled Searches

You have the option to export the completed run of a scheduled search to .csv format.

Export Search Queries and Search Criteria

You can export search queries and search criteria to a gzipped JSON file. (You must have the correct Import and Export permissions to do this.)

Build a Report Using Search Results

Search assigns a unique **Search Results ID**, which is a link to the temporary table containing the dataset that you see in the Events table and in the saved Search Results.

- You can copy the ID to build a report around those events.

- You can also build a report based on the Search Results ID for a completed run of a scheduled search.

To copy the Search Results ID for a report:

1. View the search results dataset that you want to use in the report.

2. To get the *Search ID*, click the **Copy** icon in the table's header.

3. (Optional) To view or save the copied ID, paste the ID in a text editor.

4. In the Reports Portal, complete the steps for building a dashboard or report based on the dataset.

Manage Searches

Select **Search** > **Search *<saved_search_type>***.

If you have saved a search query, criteria, or dataset, you can manage the saved items individually or in bulk; import and export search results in a CSV file; or delete them.

Manage Your Search Queries

Select **Search** > **Search Query**.

The saved search queries contain only the specified query expression, ready for you to load into a new search at any time. The list of saved queries includes both the queries that you have saved and the built-in System queries.

If you have the *Import and Export Search Queries* permission, you can **import** or **export** one or more query to a JSON file.

- Modify and Delete

- Import

- Export

Modify and Delete

You can modify or delete your queries at any time. However, you cannot delete or edit a System query. Rather, to change a System query, you should clone it, then make and save your changes.

Import

You can import a search query as a gzipped JSON file. An imported file cannot exceed 100 MB, and must contain only search queries with valid information.

1. Select **Search** > **Home** > **Search Query**.

2. Click the **Import** icon.

3. Browse to the desired file.

4. Click **Import**.

Export

You can export one or more queries to a gzipped JSON file. Click the **Export** icon.

Manage Your Search Criteria

Select **Search** > **Search Criteria**.

Saved search criteria combine a query expression and other Search elements such as fieldsets and the time range of the data you want to retrieve. The list of saved criteria includes both the criteria that you have saved and the built-in System criteria. You can **modify** or **delete** your criteria at any time. However, you cannot delete or edit a System criteria. Rather, to change a System criteria, you should clone it, then make and save your changes.

By default, search criteria are sorted alphabetically by name. Maximum search results and date fields (such as search expiration) are stored as part of the search criteria, as indicated by a message from the application. They are displayed in the **Manage Search** table, where you can visualize saved the search criteria.

If you have the *Import and Export Search Criteria* permission, you can **import**, **clone**, or **export** one or more criteria to a JSON file.

Import

1. Select **Search** > **Home** > **Search Criteria**.

2. Click the **Import** icon.

3. Select the gzipped JSON file (or files) that you want to import.

4. Click the **Import** icon.

Clone

1. Select **Search** > **Home** > **Search Criteria**.

2. Select the criteria entries that you want to clone.

3. Click the **Clone** icon.

The selection is copied with a new name, for example, entityName becomes entityName (1).

Export

1. Select **Search** > **Home** > **Search Criteria**.

2. Select the entries that you want to export.

3. Click the **Export** icon.

Manage Your Search Results

Select **Search** > **Search Results**.

When you save search results, Search stores the dataset until the search expires or you delete it from the saved list. You can sort the list by the search's name, query, event time stamp, or date of the search.

If you load the saved dataset in a Search tab, you can update the query and criteria as needed, then save those changes as a new search query, criteria, or results. Note that for a real-time search, you cannot save the query.

You can share the results with colleagues. Export all of the results to a .csv file, or share a single event as a .csv or a .pdf file.

Scheduling Regular Runs of a Search

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

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

A **scheduled search** is a search that runs on a regular interval. Whereas a saved search is saved, but does not run automatically. Each time a scheduled search runs, search adds the results to the list of Completed Searches runs.

Manage Scheduled Searches

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

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

- Create a Scheduled Search

- Manage Scheduled Searches

- Clone a Scheduled Search

- Edit a Scheduled Search

- Delete a Scheduled Search

- Enable and Disable a Scheduled Search

For your scheduled searches, you can perform the following actions:

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

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

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

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

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

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

Create a Scheduled Search

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

For every scheduled search, enter the query, fieldset, or time range for the search events or leave the defined values for the saved search. Just as for a saved search, the following considerations apply to a scheduled search:

- The search is case sensitive.

- The query input determines the search type (full text, natural language, or contextual).

- The system treats a comma (,) between search items and values as an OR operator.

- As you specify the search criteria, the system suggests search items and operators based on a schema data dictionary. To view the predefined queries, type **#** in the **query** field.

- To search for a field without data, enter [field_name] = *Null*.

To create a scheduled search:

1. Select **Search** > **Scheduled Searches**.

2. Select **+**.

3. Specify a **Name** that is 5 to 255 character long.

4. To enable the scheduled search, select **enable**.

   You also can enable and disable scheduled searches at any time in the **Scheduled** tab.

5. To indicate how frequently you want the search to run, specify one of the following options:

   - **Hourly**

   - **Daily**

   - **Weekly**

   - **Monthly**

6. Configure the settings for the dates and times of each run, based on how frequently they will run.

   Scheduled searches can run multiple days per week. These weekly searches can run once per day, at a particular hour, or they can run periodically every *N* number of hours during chosen days of the week. Additionally, you can schedule searches to run multiple times per month, as desired.

   > **NOTE:** If you choose the **End after** option, the maximum number of instances is 1000.

7. For **Search Query and Metadata**, complete one of the following actions:

   - To use an existing search, type # then select from the list of available saved searches.

   - To create a new search, specify the query, fieldset, and time range.

8. Select **Schedule**.

Clone a Scheduled Search

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

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

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

1. Select the scheduled searches that you want to clone.

2. Click the **clone** icon.

Edit a Scheduled Search

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

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

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

1. Select **Search** > **Scheduled Searches**.

2. Select the scheduled searches that you want to edit.

3. Click the **edit** icon.

Enable and Disable a Scheduled Search

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

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

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

1. Select the searches that you want to enable or disable.

2. Select **Enable** or **Disable**.

   The **Status** column, which you can add with the *Manage Columns* option, displays the status of either **Enabled** (green) or **Disabled** (red).

Delete a Scheduled Search

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

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

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

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

Manage Completed Runs of a Scheduled Search

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

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

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

- View a Completed Run of a Scheduled Search
- Save the Results of a Completed Run
- Delete Completed Runs of a Scheduled Search
- Export Completed Runs of a Scheduled Search

View a Completed Run of a Scheduled Search

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

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

The name of a completed run represents the name of the scheduled search name plus its start date and time.

When a run is in progress, Search displays the number of events received thus far and when the last chunk of data was received. Also, a flag beside the name of a completed run indicates that the settings for that scheduled search were changed before this run.

> A completed run can fail if the global search limit is exceeded. To verify if the global search limit was reached, create a new search. If the error message: "An error occurred while creating search. Exceeding the limit of 1000 global searches." displays, then the limit was reached. Contact your Administrator to increase the search limit or delete some existing searches. If you are a SaaS customer, reach out to Support to increase the search limit. For more information about increasing search limits, see "Configuring the Deployed Capabilities" in the *Administrator's Guide for ArcSight Platform*. For ArcSight SaaS customers, contact your Customer Success team.

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

View all details for a completed schedule search

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

Sort the data in columns

To change the sort order, click the **column heading**.

Reorder columns

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

Search for a search keyword

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

Hide and display columns

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

Filter the data in columns

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

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

Create a report based on the run results

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

Save the Results of a Completed Run

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

You can save the dataset from the completed run of a scheduled search, similar to saving other searches. When you save the run results, Search renames the selected run to the name that you specify. You also can choose how long to retain the dataset in the database.

1. When viewing a completed run, select the **Save** icon.

2. Specify a name for the saved dataset.

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

   • Your choice of values for each setting might be confined to limits set by your product administrator.

   • For **Delete files after**, you can specify a value that overrides how you configured Search Expires In for your search preferences.

      For example, you prefer that searches expire within five days. But you want the dataset for this completed run to expire after 10 days.

   • (Conditional) If you have the *Never Expire Search Results* permission, you can choose **Never Expire** to retain the dataset indefinitely.

4. Select **Save**.

Upgrading to the New Search Capability

After you upgrade to the new Search capability, you might encounter minor issues with saved scheduled searches. The general workaround to prevent these issues is to save your previous results **before** the upgrade and recreate them for new search runs. Issues you might see include:

   • For completed scheduled searches before and after an upgrade, the "number of results" column may not match actual search results or equal zero. But, you can still view the actual results by opening the completed scheduled searches.

- The results of scheduled searches that contain the **eval** operator may not load properly if you are loading them in a search results tab that is already open.

Delete Completed Runs of a Scheduled Search

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

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

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

1. Select the completed runs that you want to delete.
2. Click the **delete** icon.

Export Completed Runs of a Scheduled Search

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

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

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

1. Click the **CSV** icon next to the name of the scheduled search that you want to export.
2. Alternatively, view the search, then select the **CSV** icon to export the results.

For more information about exporting, see Export the Search Results.

Checking the Integrity of Event Data

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

*You must also have the **Perform Event Integrity Check** permission to run a check.*

Select **Admin** > **Event Integrity**.

The ArcSight Database stores all collected events to support event searches and analysis capabilities for the ArcSight Platform. When investigating a security incident or hunting for threats, you expect that the search results provide valid and accurate data. However, the data that you rely on could be compromised by individuals who want to hide their activities or who maliciously change content. Data also is vulnerable to human errors, transfer errors, or loss and corruption caused by hardware or software issues. To reduce the chance of data tampering, the database enforces the immutability of events once they are stored, ensuring that not even the most privileged database administrator can modify or delete an event. You can also run an **Event Integrity Check** to validate that the event information in your database matches the content sent from the SmartConnectors. The combination of an integrity check with the database's ability to resist tampering provides you an end-to-end, long-term solution for safeguarding the events to be exactly as reported by the device where the activity was observed.

When you run the check, the system searches the database for verification events received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification events. The results of an Event Integrity Check help you identify whether event data might be compromised or incomplete. The event integrity checks can involve two different types of verification events: generated for *raw events* from SmartConnectors or for *parsed fields* from Transformation Hub. Both types of verification events can be used in the same environment for increased visibility into the integrity of the events in the database.

> **NOTE**: At this time, the Event Integrity Check searches only the events ingested from SmartConnects to the ArcSight Database and does not include events migrated from Logger.

Understand the Event Integrity Check

Depending on how you have configured your SmartConnectors and Transformation Hub, the **Event Integrity Check** can verify whether raw event data and the parsed fields within an event, respectively, currently stored in the ArcSight Database match the data collected by the connectors. The check looks for events referenced by verification events in the database. The SmartConnectors group several events into a batch, then computes a hash for each raw event in the batch. If you use Transformation Hub as a destination, it also groups events then generates a hash for the parsed fields within each event. The SmartConnector and Transformation Hub each generates a *hash of the individual hashes* to create a **verification event**. The number of events in a batch depends on how you configure the batch size setting for each connector. Note that SmartConnectors do not store the hashes for individual events.

> ArcSight SaaS does not support the ability to check the parsed fields within an event.

Figure 1 (below) shows how events flow from your data sources to the SmartConnectors, which generate the verification events for the raw events. Then Transformation Hub generates verification events for parsed fields within each event.

Figure 1. *Process for generating verification events for an Event Integrity Check*
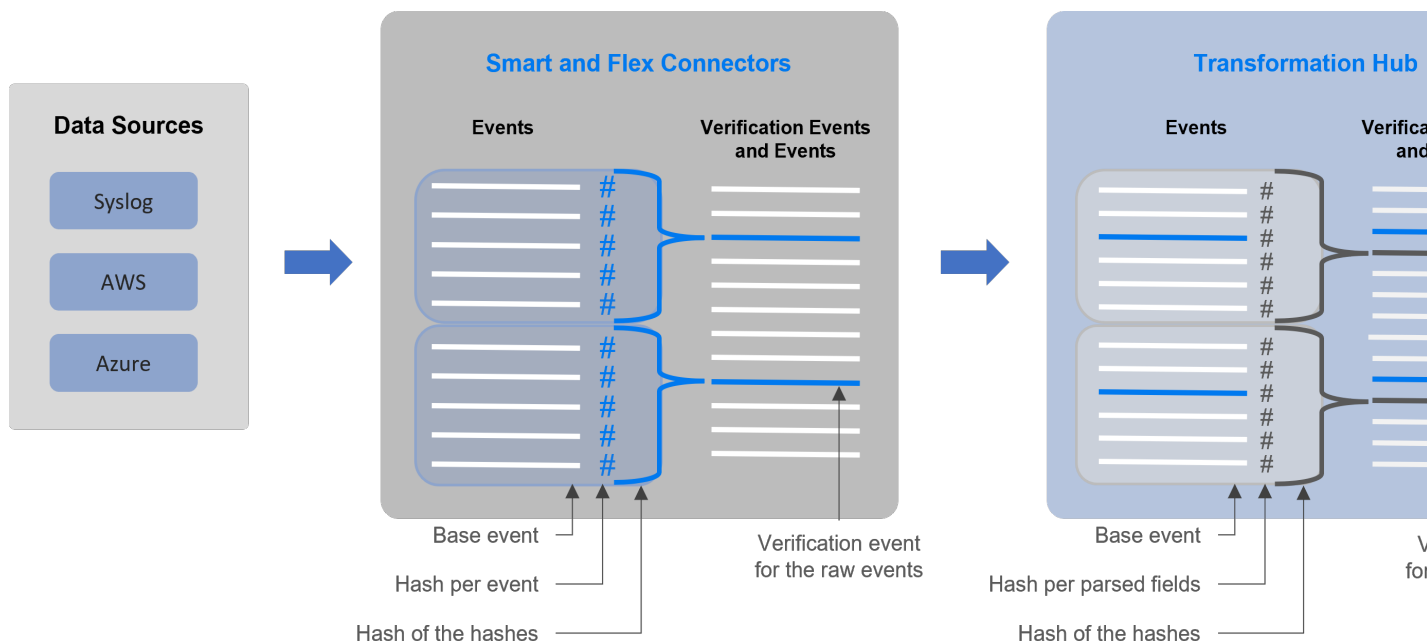
Each verification event includes the following items:

- a group of events with raw data or events with parsed fields

- an ordered list of the event IDs within the batch

- a crypto signature field representing the computed hash for that batch (the hash of hashes)

When you **run an Event Integrity Check**, the system performs the following actions for each verification event in the specified time range:

- Looks for the globally unique event ID (GEID) of each event referenced with the verification event.

- Generates hashes for the events within the base event.

- Generates a hash to represent the base events' hashes in the sequence provided by the verification event. You might call this the *generated hash of hashes*.

- Compares the generated hash of hashes to the hash of hashes in the crypto signature field that the SmartConnector or Transformation Hub created for the verification event.

> Some base events could have been deleted on purpose to comply with data retention policies, depending on how you have configured the storage groups. When performing an event integrity check, the system reports these deleted events as missing base events.

Run an Event Integrity Check

Select **Admin** > **Event Integrity**.

An Event Integrity Check looks for verification events received within the specified date range. To reduce the chance of false-negative results, the check also searches for base events outside of the specified date range. For example, you specify a date range of 29 May to 5 June. The check finds several verification events within the date range; however, Verification Event A was created on 29 May and includes base events that occurred on 28 May. To prevent the verification event from failing, the system will expand the search for base events beyond the specified dates.

You can run one check at a time only. If the **Run** button is disabled, a check is running currently. The system provides a **Status** update for the actively running check, as well as a showing when the check began and its specified date range.

> **NOTE**: The check process can take a long time if it includes large amounts of data. Therefore you should run the check during off-peak hours, and limit the date range to include only the data that you are interested in.
>
> If you are running large jobs, or if your system resources are limited, you might consider disabling the **Event Integrity Check Auto-tuning Parameter Setting** and reducing **Task Count** and **Chunk Size** values. For more information, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform 23.3*.

1. Select **Admin** > **Event Integrity**.

2. Specify the **Start Date** and **End Date** for the range of data that you want to check.

   The *Start Time* for the check corresponds to the time when you select **Run**. For example, 5:29 pm.

   > If the start and end dates encompass a time when the database is receiving events, it's possible to get a Missing Events notification. This occurs because the integrity check finds the verification events before ingesting their associated base events. We recommend that you avoid running the check against events currently being ingested by the database.

3. Select the timestamp type.

4. Click **Run**.

5. (Optional) To cancel the check, click **Cancel**.

   Run as needed.

6. View the results.

View Event Integrity Check Results

To view the status and results, select **Admin** > **Event Integrity**.

The **Event Integrity Check** feature provides the following status and results:

- View the Event Integrity Check Status

- View Last Event Integrity Check Results Table

View the Event Integrity Check Status

The **Event Integrity Check status** displays the date range from which the results are currently being checked, as well as the current status.

> If the system is busy, it might take a moment for the interface to indicate whether a check is running or has been canceled.

New

Indicates that you have never performed an Event Integrity Check; therefore, no results display.

In Progress

Indicates that an Event Integrity Check is running. If **Run** is disabled, a check is running currently. You can run one check at a time only.

Canceled

Indicates that you canceled an Event Integrity Check, and the system has completed the cancel task.

Canceling the check might take time to end the tasks that had been in progress.

Completed

Indicates that the Event Integrity Check has completed successfully. The results display in the results table.

Failed

Indicates that the Event Integrity Check failed to complete due to an error. The following table lists the failure categories and recommended remediation.

> Hover your cursor over the information icon next to "Failed" to display the corresponding error message.

For this error or warning...	Which indicates that...	You might want to...
Insufficient Disk Space...	The system does not have enough disk space either to run the check or to create a table in the database for the verification events	Run the check when the system is less busy
Insufficient Resources...	The system does not have enough memory either to run the check or to create a table in the database for the verification events	Run the check when the system is less busy
Event Integrity Running	An Event Integrity Check is already running	Wait for the current check to finish or cancel the check in progress
No events found in the specified time range	Either the events do not exist or the system cannot communicate with the data source	Check whether the SmartConnector, Transformation Hub, or Kafka Scheduler is offline
No verification events found in the specified time range	The system might not be configured correctly	Check whether SmartConnectors or Transformation Hub have been configured to support Event Integrity Checks

More than one algorithm found	The system might not be configured correctly	Ensure that only one algorithm has been specified for Event Integrity Checks in the SmartConnector and Transformation Hub
Unsupported algorithm (SHA512) found	The system is not configured correctly	Ensure that the SmartConnector or Transformation Hub have been configured to use one of the approved algorithms: MD5, SHA-1, or SHA-256
Other errors	Depends on the situation	Review the details of the error in the Search Engine log

View Last Event Integrity Check Results Table

The **Last Event Integrity Check Results table** displays the date range from the last check as well as the details of the last check, including the following information:

> The Event Integrity Check might display the last result from another user. The last result might also display after logging out.

Base events checked
Represents the number of base events referenced by verification events found in the specified date range.

Intact events
Represents the number of base events referenced by verification events that passed the Event Integrity check.

Missing events
Represents the number of base events referenced by verification events where missing base events exist.

> You might see this result when the integrity check finds the verification events before ingesting their associated base events. Try adjusting the start or end date for the check.

Tampering has been detected
Represents the number of base events referenced by verification events where the Event Integrity check failed to match the information provided by the verification events, such as due to a change in the data in the base event.

Missing hashes, incorrect hashes, or base events being out of sequence usually indicates that the data has been deliberately changed in an attempt to hide a user's activities.

Duplicate base event IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one base event has the same globally unique event ID. This situation results in the Event Integrity check of the referenced base events to fail.

Duplicate verification events IDs

Represents the number of base events referenced by verification events where the Event Integrity check failed because more than one verification event has a globally unique event ID.

Configure Data Collection to Support Event Integrity Checks

An Event Integrity Check can review both raw event data and the parsed fields within an event, depending on how you configure SmartConnectors and Transformation Hub, respectively.

Configure a SmartConnector to Generate a Verification Event

The Event Integrity Check can verify the raw data received from a SmartConnector. You must configure the connector to generate a verification event for batches of events. This configuration allows you to verify that the raw data in the database matches the event captured at the moment that it occurred in your environment.

To configure a SmartConnector, complete the steps for your environment:

- Non-SaaS environment, see Configuring a SmartConnector to Include a Verification Event for Raw Events in the *Administrator's Guide to ArcSight Platform 23.3*.

- SaaS environment, see "Configuring a SmartConnector to Include a Verification Event for Raw Events" in the *Quick Start for Administrators*.

Enable Transformation Hub to Generate Verification Events for Parsed Fields

ArcSight SaaS does not support the ability to check the parsed fields within an event.

The Event Integrity Check can verify the integrity of multiple parsed fields within an event that Transformation Hub received from a SmartConnector. For example, it verifies the *deviceProduct* and *sourceHostName* fields if they exist in an event. You might want to check these types of parsed fields as an alternative to verifying the raw event data. For example,

your environment might not have the disk space, processing power, or network capacity to manage large amounts of raw event data forwarded from SmartConnectors.

You can configure this setting as you deploy Transformation Hub or at any time after deployment. For more information, in a non-SaaS environment, see Enabling Transformation Hub to Generate Verification Events for Parsed Fields in the *Administrator's Guide to ArcSight Platform 23.3*. The SaaS environment does not currently support checks of parsed events.

Analyzing Anomalous Data with Outlier Analytics

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability . *Requires the Manage Outlier Models and Scoring permission.*

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.

Generating Models to View Anomalous Data

You must have the Manage Outlier Models and Scoring permission 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

- Define and Build a Model

- Score a Model

- Delete a Model

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, we recommend 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.

Define and Build 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.

The feature then calculates a sum for:

- *EventCount*

- *BytesIn*

- *BytesOut*

Outlier Analytics then creates conditional probability tables for sum of *EventCount*, sum of *BytesIn*, and sum of *BytesOut*.

To build a model:

1. Review the considerations for building a model.

2. Select **Configuration** > **Outlier**.

3. From the **Create Model Configuration** section, 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 more easily find the model later, give the model a name by typing over the **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. For the time range, perform **one** of the following actions:

   - Accept the default time (**Last 14 days**)

   - From the menu, select a pre-defined value under **Quick Ranges**

   - From the menu, use the **Custom Range** fields to specify a time range

   - From the menu, select **Dynamic**, and then enter a dynamic date value

   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. Click **Create**.

   The created model displays 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. Click **Build**.

9. To evaluate incoming events against the model, you must start the scoring process.

Score a Model

*You must have the **Manage Outlier Models and Scoring** permission 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**.

Delete a Model

*You must have the **Manage Outlier Models and Scoring** permission 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. From the **Available Models** table, select the model that you want to delete.

3. Click **Delete**.

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, point to the corresponding area in the chart.

Selected Anomalous IP

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

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

Investigate Anomalies Further

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. Specify a valid time range to view the scored data.

    The 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**.

5. Click **Detect**.

    > If the scored model does not return data, the global search limit may have been reached. To verify, create a new search. If the following error message displays: "An error occurred while creating search. Exceeding the limit of 1000 global searches." displays, then the limit was reached. Contact your Administrator to increase the search limit or delete some existing searches. If you are a SaaS customer, reach out to Support to increase the search limit. For more information about increasing the search limit, see Configuring the Deployed Capabilities in the *Administrator's Guide to ArcSight Platform 23.3*.

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

    > ⚠ **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 click **Play** 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:

    a. Right-click a row in the grid.

    b. Select **Search for <IP_Address>**.

Using Visuals and Reports to Analyze Data

Your environment must include a capability that uses the reports.

The **Reports Portal** allows you to browse and filter your datasets and to visualize results in the Portal's reports and dashboards. Rapidly discover meaningful trends and associations that yield actionable intelligence. The built-in Admin reports enable a report administrator to track use of the Portal.

If your product provides built-in reports and dashboards, you usually can find them in the *Standard Content* directory of the Portal's repository. Depending on your assigned permissions, you can view, schedule, design, or manage reports and dashboards. You add custom reports and dashboards by collecting and filtering data from your connected sources. The Reports Portal supports the ability to drill down into specific elements for thorough data reviews.

Accessing Reports and Dashboards in the Reports Portal

Your environment must include a capability that uses the Reports Portal. Also, you must have one of the Reports permissions to use this feature.

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 out-of-the-box 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.

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.

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 that 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 specify the time range, complete the following steps:

   a. To activate the Calendar, point your cursor at the position of the **Calendar** icon to the right of the time selection box.

   b. Select the **Calendar** icon.

   c. Enter the **Start Time** for the report.

   d. 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 **Schedule**, then define the delivery options.

Specify 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 OWASP Missing Security Patches Overview and Foundation Denial of Service Activity 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 (?).

Customize Your Dashboards

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

You can customize the features of some built-in dashboards as well as the ones that you create. For example, a built-in dashboard might allow you to specify a particular time range. Some charts in your dashboards also allow for customization.

- Change the Default Time Frame of a Dashboard
- Customize Charts in a Dashboard

Change the Default Time Frame of a Dashboard

You can change the time range for some built-in dashboards, as well as those you create.

1. In the Reports Portal, navigate to the dashboard that you want to modify.

2. Right-click the dashboard, click **Edit**.

3. Select **Options**.

4. Select **Scripts**.

5. Change the default value of the following parameters:

- parameter.start_time

- parameter.end_time

For example:

To change the default start time to the past three hours instead of the past two hours, change the time as follows:

from

```
startTime.setHours(startTime.getHours() - 2);
```

```
parameter.start_time = startTime;
```

to

```
startTime.setHours(startTime.getHours() - 3);
```

```
parameter.start_time = startTime;
```

Customize Charts in a Dashboard

Some charts can be customized in the following ways:

Any chart

- The table at the bottom of each dashboard displays individual events and associated information, such as severity, source address, and destination address. To view a particular event in the Event Inspector, click the left-most icon of the row for the event.

- You can adjust the filters to include or exclude information.

- To investigate and filter the displayed data, use the **Open in Search** option to start a query based on the data in the dashboard.

Bar chart
Organize results from the highest or lowest amounts. For example, show the *Top Target IPs*. You also can choose the amount of results displayed: 10, 25, 50, 100.

Parabox charts
Visualize connections between multiple entities and identify significance based on the size of target elements, such as source user.

Timeline chart
Display events by hour or minutes.

Word Cloud charts
Display data according to key words, based on the chart's purpose.

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 using the bundled Standard Content data worksheets. 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.

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.

> The system automatically saves scheduled tasks regardless whether you close the task or click **OK**.

Adding and Removing Reports Content

*You must have the **System 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.

When exporting reports, it is recommended that:

- You uncheck the **Overwrite assets of same name** option so you do not accidentally overwrite assets of the same name on the target systems; unless you are sure you want to overwrite existing assets of the same name on the target system.

- You uncheck the **Required Assets Included** option as an extra precaution not to accidentally overwrite assets of the same name on the target systems. Only include any new assets that you created with your new report. This way, even if the end user checks the **Overwrite assets of same name option** when importing the report, they won't accidentally overwrite their base assets.

Please review the following considerations for importing and exporting content:

- You cannot export content from the My Reports folder.

- If Reporting generates errors when you attempt to export assets, you should reduce the number of assets that you export concurrently.

- ArcSight SaaS users are not allowed to import or modify Data Sources, Logical Models, or Virtual Private Models.

- On non-SaaS systems, only users with the System Admin role are allowed to import and modify Data Sources, Logical Models or Virtual Private Models.

Supported Data Sources

This capability is not available in the Arcsight SaaS environment.

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.
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.

Best Practices for the Report Designer and Dashboard Designer

When using the Reports Portal, follow these best practices to improve your work flow for creating reports and dashboards.

Use Search Results to Create a Dashboard or Report

Each completed search has a unique **Search Results ID**, which represents a link to the temporary table containing the search results. You can copy that ID, then build a report or dashboard around the search results.

- Build a Report Using Search Results
- Build a Dashboard Using Search Results
- Convert the Search Fields to Human-Readable Values

Build a Report Using Search Results

You can build a report around results of a previously run search by leveraging the Search Results ID.

1. When viewing the Events table for a search, select the **Copy** icon in the table's header.

    This icon contains the **Search Results ID**.

2. Select **Reports** > **Report Designer**.

3. Select **Create** > **Report**.

4. In the **Select a data source** field, paste the Search Results ID that you copied.

    The retention period of the temporary table in the database is 30 days.

5. (Optional) Convert the fields in the temporary table to human-readable values.

6. Continue creating the report.

Build a Dashboard Using Search Results

You can build a dashboard around results of a previously run search by leveraging the Search Results ID.

1. When viewing an Events table, select the **Copy** icon in the table's header.

    This icon contains the **Search Results ID**.

2. Select **Reports** > **Dashboard Designer**.

3. Select **Create** > **New Dashboard**.

4. From the visual composer, select **Data Source** > **Database** > **TABLE** > **Default_secops_ recon**.

5. Select the ID of the search that you previously copied.

    The retention period of the temporary table in the database is 30 days.

6. Select **Open wizard** or **OK**.

7. (Optional) Convert the fields in the temporary table to human-readable values.

8. Continue creating the dashboard where the Search Results ID is the data source.

Convert the Search Fields to Human-Readable Values

The ArcSight Database uses a temporary table to store content associated with a Search Results ID. Because the names of the fields in the table represent the coding-style name, you might want convert the terms to more user-friendly values.

To change the field names, your report or dashboard must use a Data Worksheet.

1. Select **Reports** > **Dashboard Designer**.

2. Open the dashboard or report that you want to modify.

3. From the upper-right corner, select the **Data** icon.

4. Open the worksheet.

5. In the lower pane, select the **Formula Editor** icon. The tool-tip for this icon says "Create Expression."

6. Select **SQL**.

7. In the Expression pane of the Formula Editor, add the following strings:

```
Time: to_timestamp(field['normalizedEventTime']/1000)
IP:   v6_ntoa(field['sourceAddressBin'])
MAC:  mac_btoa(field['sourceMacAddressBin'])
```

8. Select **OK**.

9. In the lower pane of the worksheet, select the **Change Data Mode** icon.

10. Select **Live Event** data.

11. Hide the binary (original) fields.

12. **Export** or **Save** the dashboard or report as needed.

Use Data Models to Build a Worksheet

Select **Reports** > **Reports Designer** > **Report type** > **Data Source** > **Database**.

Data models are logical models of the events table in the database that allow for an extra level of abstraction where you can perform varied transformations. You can use the final data model as the final table when creating a data worksheet. By default, the system has two data models:

Basic Data Model
Contains fewer fields from the events table. Use this model for an easier understanding or for simple reports that require less fields.

Event View
Contains the entire events table.

You can also create, edit, and delete your own Data Models. For more information, see "Create a Data Model" in the Help in the Reports Portal. Make sure to add only the fields you that need and create the filters from there. Some of the fields in the data model are non-human readable. You should parse them to ensure that they are readable in the report.

Use Data Worksheets to Build a Dashboard or Report

Data worksheets define the base for the reports and dashboards. Using data worksheets allows you to freely manipulate different data origins and generate a final set of results that can be used for reports and dashboards.

1. Select **Reports** > **Dashboard Designer** or **Report Designer**.

2. From the upper-right corner, select the **Data** icon.

3. From the right corner, select the **New Data Worksheet** icon.

4. To start the worksheet, complete one of the following actions:

   4a (Conditional) To browse for a data source, select **Database Query**, then **OK**.

   4b (Conditional) To import a data file, select **Upload File**, then **OK**.

   4c (Conditional) To open a new worksheet then choose the data source, select **Mashup Data**, then **OK**.

   4d (Conditional) To open a new worksheet, select **Cancel**.

5. Drag and drop the fields, tables, or queries that you want to include in the dashboard or report.

   Alternatively, you can create tables, then link them using unions or joins.

   > Using joins to show correlations between data sources like CSV files and event charts might cause slow performance depending on the size of the files. For larger data sources, see Use Pre-Populated Search Results.

6. (Conditional) To refine the design, select one of the following options from the Preview pane.

   For example, you can sort and reorder the columns or change the data mode.

   > Be sure to hide or remove fields that you don't need for your dashboard or report.

7. To save your changes, complete the following steps:

   7a Select **Save** or **Save As**.

   7b Specify the folder where you want to save the worksheet.

   Do not specify the **Standard Content** folder, which is reserved for the built-in reports and dashboards.

> When you create a custom report, do not base that report on any existing **Standard Content** DataWorksheet. Instead, create a new DataWorksheet or use the DataSource/table selection options.

Create a Simple Dashboard

When creating a simple dashboard, Reports prompts you to select the data source. When you open the Dashboard Visual Composer, a window displays where you can choose the data source for the Dashboard. Follow the prompts or close the window to continue to the main editor of the Dashboard.

From the Dashboard editor, you can create Tables and Charts in the canvas. From there, you can also convert to measure some fields that can provide numeric values and can be used in a chart. You can also convert to dimension the fields that can provide a string value.

First, use the system to create and save a data worksheet as the basis for your dashboard. Use one of the following to create a simple dashboard.

- Use the Dashboard Wizard
- Use the Dashboard Editor

Use the Dashboard Wizard

If you select the wizard, the Dashboard Designer displays the Wizard section of the Dashboard. From here, you can create the first component of the Dashboard.

1. Select **Reports** > **Dashboard Designer** > **Crosstab Wizard**.

2. Select the **data worksheet** of your preference as a data source, and then click **Next**.

3. Select **Open Wizard**.

4. Select the fields to use in your dashboard.

5. (Conditional) Select the dashboard style:

   Crosstab

   Groups the dashboard by row and column headers and displays the summary data at the intersections

   Table

   Groups the dashboard and summarizes it or displays it in tabular layout

   Chart

Creates multiple charts using multiple fields

Full Editor

Allows granular control view of your updates, such as format, color, and shape

6. Once the editing is complete, set the position of the element in the dashboard canvas.

7. View the dashboard, and then select **Continue**.

8. Once the dashboard has been successfully edited, select **Finish**.

9. Click **Save as** to save your dashboard.

Use the Dashboard Editor

Using the Dashboard Designer, you can edit the elements and freely set their position in the Dashboard. The Dashboard Designer displays the Wizard section of the Dashboard.

1. Select **Reports** > **Dashboard Designer** > **Crosstab Wizard**.

2. Click **Cancel** to open the dashboard editor.

3. Select the **data worksheet** of your preference as a data source, and then click Next.

4. Add the elements available from the left.

5. Update the dashboard using the Dashboard composer.

   You can create, add, and edit multiple elements.

6. Click **Save** to save your dashboard in a **Custom Content** folder.

Create a Parabox Chart

Parabox charts, also called Parallel Coordinates, allow you to visualize connections between multiple entities and identify significance based on the size of target elements. This allows you to quickly discover threats and respond to suspicious activity in your environment.

1. Select the **Create New** icon.

2. Choose the data source.

   Make sure the data source includes the fields you want to represent on the parabox chart.

3. When the visual composer opens, drag the chart from the left panel.

4. Select the **Edit** icon.

5. Select **Full Editor**.

6. Drag the fields you want for the Y axis to the box labeled **Y**.

7. Right click on the Y axis.

8. Select **Hide Title**.

9. Right click on the chart.

10. Select **Properties** .

11. Select **Script**.

12. In the **Script** section, paste the code below.

```
if(this.data.length>1){
        //new EGraph() creates a new instance of a EGraph object and
represents the graph definition
        graph = new EGraph();
        //Create a new Parabox element
        var elem = new ParaboxElement();
        //Obtain fields and ordering from binding dialog instead of
having to declare them
        var y =  bindingInfo.yFields;
        var scales = [];
        for(var j=0; j < y.length; j++) {
                var z = new CategoricalScale(y[j]);
                //hide line
                z.getAxisSpec().setLineVisible(false);
                //add categoricalScale to array
                scales.push(z);
                //Add the required fields to the parabox.
                elem.addParaboxField(y[j])
                }
                var coord = new ParaboxCoord(scales[0],scales[1]);
                coord.setScales(scales);
                //set vertical spacing between data points; default is 10,
requires build 143798+
                //coord.setSpacing(15);
                //Set the Font and Color of the column labels
                var labelColor = coord.getAxisLabelScale().getAxisSpec
().getTextSpec();
                labelColor.setFont(java.awt.Font
('Roboto',java.awt.Font.PLAIN, 10));
                labelColor.setColor(java.awt.Color(0xFFFFFF));
                //Sets the graph coordinates to the Parabox Coordinates
defined above
                graph.setCoordinate(coord);
                //Create new Text Specifications to set the text format of
the points
```

```
                    var pointColorFont = new TextSpec();
                    pointColorFont.setFont(java.awt.Font
('Roboto',java.awt.Font.PLAIN, 11));
                    pointColorFont.setColor(java.awt.Color(0xFFFFFF));
                    elem.setTextSpec(pointColorFont);
                    //set shape and color of data points
                    var sframe = new StaticShapeFrame();
                    var cframe = new StaticColorFrame();
                    cframe.setColor(java.awt.Color(0x0073E7));
                    sframe.setShape(GShape.FILLED_CIRCLE);
                    elem.setShapeFrame(sframe);
                    elem.setColorFrame(cframe);
                    //set connecting line color
                    var cframeLine = new StaticColorFrame();
                    cframeLine.setColor(java.awt.Color(0x44495B));
                    elem.setLineColorFrame(cframeLine);
                    //Add the parabox element to the graph
                    graph.addElement(elem);
                    }
```

13. Select **Apply**.

Create a Simple Scheduled Report

You can create a report that runs on your chosen schedule. In the report, define conditions
that trigger tasks and actions you want to run.

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

2. In the lower left corner of the screen, select **New Task**.

3. For **Name**, enter a name of the task.

4. To set the conditions for your report, complete the following steps:

   a. Select the **Condition** tab.

   b. (Conditional) To specify the timezone that the report uses, perform one of the
      following actions:

      • To use the timezone where the server is installed, select **Show Server Time
        Zone**

      • To use your timezone, deselect **Show Server Time Zone**

   c. (Conditional) To run the task at specific intervals, configure the frequency.

For example, to run a report every Monday afternoon, specify the following settings:

- Select **Time Range**, then **Afternoon**

- For **Every**, enter 1

- Select Monday

d. (Conditional) To run the tasks in sequence, select **Chained**, then specify the first task.

e. Select **OK** to save the scheduled task.

> The system automatically saves scheduled tasks even when you close the task rather than clicking **OK**.

5. To specify the report associated with the scheduled tasks, complete the following steps:

a. Select the **Action** tab.

b. For **Report**, click **Select** then navigate to the report that you want to schedule.

c. To email the report results, select **Deliver to Emails** then configure the email content and destination addresses.

d. To set the time range in which the report retrieves data, complete one of the following actions:

- Select **Add**, and then specify the time values.

- Select **Creation Parameters**, then choose the dates from the calendar option.

e. Select **OK** to save your changes.

Create a Simple Report

First, create and save a data worksheet. For additional details on how to create a data worksheet, see Using Data Worksheets to Build a Dashboard or Report.

Use the one of the following wizards to create a simple report.

- Use the Crosstab Wizard

- Use the Table Wizard

- Use the Chart Wizard

- Guidelines for Report Usage

Use the Crosstab Wizard

From the Reports Designer menu, use the Crosstab Wizard to create a report that displays data in a pivot table where the data is grouped by row and column headers, and the summary data is displayed at the intersections.

1. Select **Reports** > **Report Designer** > **Crosstab Wizard**.

2. Select the **data worksheet** of your preference as a data source, and then click **Next**.

3. Define the **row and column groups** (vertical and horizontal columns), and then click **Next**.

   - For **Row groups**, select the row headers.

   - For **Column groups**, select the column headers.

4. (Conditional) Define the **summary columns** that will display as summarized fields.

5. (Conditional) **Filter the conditions** that will define the original data.

   After the design statement is filled, the options for insert, modify, and clear will be enabled.

6. (Conditional) For **table style**, use the default option.

7. To complete the editing, click **Finish Editing**.

Use the Table Wizard

From the Reports Designer menu, use the Table Wizard to create a report that displays data in tabular layout or grouped and summarized.

1. Select **Reports** > **Report Designer** > **Table Wizard**.

2. Select the **data worksheet** of your preference as a data source.

3. Select the columns to display in the report from the select **detail columns**.

4. Define the groups to display as **column headers**.

5. (Conditional) Define the **summary columns** that will display as summarized fields.

6. (Conditional) Filter the conditions to define the original data. Once the design statement is filled, the control options are enabled.

7. (Conditional) Retain the default **table style** for better formatting results.

8. (Conditional) Rank the groups to display as top or bottom groups.

Use the Chart Wizard

From the Reports Designer menu, use the Chart Wizard to create a chart-based report.

1. Select **Reports** > **Report Designer** > **Chart Wizard**.

2. Select the **data worksheet** of your preference as a data source.

3. By default, the auto option is selected. Use the **chart style** to style your report.

4. (Conditional) If required, select one of the following 2D and 3D images chart styles.

   Your chart options include bar, line, area, point, pie, donut, radar, stock, candle, box plot, waterfall, pareto, map, treemap, and marimeko charts.

5. Define the **X Axis** that to display as columns.

6. Define the **Y Axis** to display as columns.

7. Define the visual properties (color, shape, size, text) of the columns by using the visual binding.

8. (Conditional) Filter the conditions to define the original data. Once the design statement is filled, the control options are enabled.

   (Conditional) Rank the groups to display as top or bottom groups.

9. (Conditional) Additional steps might be required depending on the chart style selected:

   Geographic binding

   Use if you select **Map Style** for your report. Choose different aspects about the map report that will be generated.

   Tree dimensions

   Use if you select **Treemap**, **Sunburst**, **Circle Packing**, or **Icicle** for your report. Select the fields
   the report will use for the Tree Mapping.

   Marimekko category

   Use if you select **Marimekko Style** for your report. Select the field for the Marimekko Category Dimension.

Guidelines for Report Usage

- Create as many data models as needed but only include the fields that you need for your report. For simple reports, use the Basic Data Model instead of the event view.

- To convert non-human readable fields in the data model, parse them before adding them to the report.

- You can create filters from the data model or the report itself. It is recommended to set the filters from the data model so these can be saved in the data base.

- Check the meta data box for a faster pre-visualization of the report. Take into consideration that no real data is displayed with this option.

- Export the results in CSV format for faster results.

- When needed, copy the built-in dashboards and use them as templates for other creations.

Improve the Performance of Dashboards and Reports

You can improve the performance of your reports, dashboards, and worksheets by following these best practices.

- Use Raw Database Fields instead of Defined Functions Fields
- Use `normalizedEventTime` Instead of the Time Field
- Use the Integer Variant Instead of the String Variant
- Display Host Names Instead of IP Addresses on Charts
- Use `startswith` or `endswith` Instead of `contains` to Create Conditions
- Put the Expensive Conditions at the Top of your Worksheets
- Put the Most Expensive Conditions Towards the Top of your Building Blocks Hierarchy
- Put Parameters at the Top of your Worksheets
- Use the Flyover Option for Dashboards with Multiple Charts and Tables

Use Raw Database Fields Instead of Defined Functions Fields

Where possible, use raw database fields over defined function fields to speed up the search process by limiting the number of events searched.

icons represent the defined function fields. icons represent the raw database fields.

For example, use: `[Events.deviceAddressBin][is not][null]` instead of `[Device Address][is not][null]`.

Use Normalized Event Time Instead of the Time Field

Use `normalizeEventTime` instead of the **Time** field from the logical model. Because the **Time** field requires extra calculations, whereas `normalizeEventTime` is a raw field, your query will run more quickly. For more information, see Use Raw Database Fields instead of Defined Functions Fields.

Use the Integer Variant Instead of the String Variant

When data can be represented in a string format or an integer format, use the integer format of the data field because strings are defined functions and integers are raw database fields. For more information, see Use Raw Database Fields instead of Defined Functions Fields.

For example, use: `[Events.agentSeverity][is][one of][3,4]` instead of `[Events.Agent Severity String][is][one of][High,Very-High]`.

Display Host Names Instead of IP Addresses on Charts

Where possible, use host names because host names are represented as raw fields in the database. IP addresses represented as database function `v6_ntoa(Events1_0.destinationAddressBin) AS Target Address` will be calculated for every selected event.

Use 'startswith' or 'endswith' instead of 'contains'

To create conditions, use `startswith` or `endswith` instead of `contains`, when possible. This narrows your search, and your queries will process more quickly.

For example: `[Events.categoryTechnique][is][starting with][/Traffic Anomaly]`.

Put the Most Expensive Conditions at the Bottom of Your Worksheets

When you have conditions that take up a lot of operation space, put them at the bottom of your worksheet. This will limit the quantity of events that the expensive condition must search, and thus speed up your query.

Put the Most Expensive Conditions Towards the Top of Your Building Blocks Hierarchy

For advanced users.

When you need to display expensive conditions on your dashboard, you can move it up in the hierarchy. This improves your dashboard's performance because those conditions will not run against every event.

> **Note:** This does not work for reports, only dashboards.

> ⚠️ **Caution:** If you have a wrapper function and move it up the in the hierarchy, you need to define the wrapper function multiple times. For example, if you have multiple charts showing the same field from different angles (one chart is Top Target IPs, and another chart for relationships between attacker IPs and Target IPs) you will need to define the wrapper function twice.

Put Parameters at the Top of your Worksheets

If you create a dashboard or report with parameters (for example, data for a specific host), arrange the worksheet conditions so that the parameter goes before the complex conditions. This will limit the events that the complex conditions search and speed up your query.

For example:

```
[Events.destinationHostNamelowerCase][is][contains][$(hostname(equal_or_
like))]
```

`[and]`

```
[Events.Time][is][between][$start_time.$(end_time)]
```

Use the Flyover Option for Dashboards with Multiple Charts and Tables

When you have a dashboard with a table, consider using the flyover option instead of using the charts and tables on one screen. If you designed the dashboard with the flyover option, the dashboard will show one chart. When you click on a specific target, a flyover table will show the information for this specific target. Right-click the dashboard you want to use the flyover option.

1. Select **Properties**.

2. Under **Flyover**, click the box or boxes for the additional chart or table you want to appear, and then click **OK**.

Additionally, when you again pause the mouse over the specific target, the flyover information appears more quickly because it is drawn from the cache.

When to Write your own SQL Query

If you want to run a very specific query, and you do not want to use the logical model, you can write your own SQL query.

1. From New Data Worksheet, select Database Query.

2. Add fields.

3. Write your SQL query, save it, and use it like any other worksheet. For more information, see Use Search Results to Create a Dashboard or Report.

Hunting for Known Threats and Vulnerabilities

Available only with ArcSight capabilities.

To help you hunt for undetected but industry-recognized threats and vulnerabilities, 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 the Cloud Security Alliance and OWASP. Additional reports and dashboards focus on fundamental security issues, such as monitoring firewalls and malware.

For rapid access to your regular dashboards, you can configure the Reports Portal to display your preferred dashboards by default. For some dashboards, you also can customize the date and time of a dashboard by adjusting the **Start** and **End** times. By default, the system displays events from the past two hours.

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). This alliance has identified the most significant security threats to the shared, on-demand nature of cloud computing. CSA refers to these issues as the **Treacherous 12**.

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

Category	Dashboards	Reports
Abuse and Nefarious Use of Cloud Services	DoS Originated from EC2 Instances EC2 Instances Communicating with Cryptocurrency Entity EC2 Instances Querying Domains Involved in Phishing Attacks EC2 Machines Involved in Suspicious Communication Email Spam Originated from EC2 Instances Nefarious Activity by an Unauthorized Individual from EC2 Suspicious Activity Reported by Microsoft Azure Trojans or Backdoors Installed on EC2 Instances	n/a
Account Hijacking	Account Hijacking Vulnerabilities Man in the Middle Attacks Phishing Attacks Principal Invoked an API Commonly used to Discover Information Associated with AWS account	Broken Authentication and Session Management
Advanced Persistent Threats	Trojans or Backdoors Installed on EC2 Instances	n/a
Data Breaches	All Information Leakage Events Information Disclosure Vulnerabilities Organizational Information Leakage Personal Information Leakage	n/a
Data Loss	Amazon AWS Deletion Events	Amazon S3 Bucket Deletion Events 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 Failed Technical Compliance Events

Category	Dashboards	Reports
Insufficient Identity Credential and Access Management	n/a	AWS Account Password Policy Was Weakened Invalid or Expired Certificate Unsecured Password Events
Malicious Insiders	n/a	Nefarious Activity by an Unauthorized Individual
System Vulnerabilities	Vulnerability Overview	Cloud Related Vulnerabilities Critical Vulnerabilities Heartbleed Vulnerabilities Kernel Vulnerabilities Overflow Vulnerabilities Security Patch Missing Shellshock Vulnerabilities Spectre and Meltdown Vulnerabilities Vulnerabilities by Host
Vulnerabilities on Shared Technologies	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 the ArcSight Database 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

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.

Dashboards	Reports
DoS Originated from EC2 Instances	n/a
EC2 Instances Communicating with Cryptcurrency Entity	
EC2 Instances Querying Domains Involved in Phishing Attacks	
EC2 Machines Involved in Suspicious Communication	
Email Spam Originated from EC2 Instances	
Nefarious Activity by an Unauthorized Individual from EC2	
Suspicious Activity Reported by Microsoft Azure	
Trojans or Backdoors Installed on EC2 Instances	

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 is 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

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.

Dashboards	Reports
Account Hijacking Vulnerabilities Man in the Middle Attacks Phishing Attacks Principal Invoked an API Commonly used to Discover Information Associated with AWS Account	Broken Authentication and Session Management

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

Man in the Middle Attack
> 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 organization.

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

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.

Dashboards	Reports
Trojans or Backdoors installed on EC2 Instances	n/a

Trojans or Backdoors Installed on EC2 Instance

Provides charts showing backdoors or trojans discovered on EC2 (AWS Elastic Compute Cloud service) machines.

Data Breaches

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:

Dashboards	Reports
All Information Leakage Events	n/a
Information Disclosure Vulnerabilities	
Organizational Information Leakage	
Personal Information Leakage	

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

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

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

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

Data Loss

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.

Dashboards	Reports
Amazon AWS Deletion Events	Amazon S3 Bucket Deletion Events
	Amazon VPC Deletion Events

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

Amazon AWS Deletion Events
Provides charts and a table listing the number of deletion events by operations, day, source address, and source user.

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.

Denial of Service

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.

Dashboards	Reports
DoS Activity	

DoS Activity
Provides charts 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

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.

Dashboards	Reports
n/a	Vulnerabilities on Interfaces and API

Vulnerabilities on Interfaces and API
Reports the vulnerabilities found in your cloud-based interfaces and APIs.

Insufficient Due Diligence

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.

Dashboards	Reports
n/a	EC2 Machines Behavior Deviates from the Established Baseline
	Failed Technical Compliance Events

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

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.

Dashboards	Reports
n/a	AWS Account Password Policy Was Weakened
	Invalid or Expired Certificate
	Unsecured Password Events

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

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.

Dashboards	Reports
n/a	Nefarious Activity by an Unauthorized Individual

Nefarious Activity by an Unauthorized Individual
> 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

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.

Dashboards	Reports
Vulnerability Overview	Cloud Related Vulnerabilities
	Critical Vulnerabilities
	Heartbleed Vulnerabilities
	Kernel Vulnerabilities
	Overflow Vulnerabilities
	Security Patch Missing
	Shellshock Vulnerabilities
	Spectre and Meltdown Vulnerabilities
	Vulnerabilities by Host

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 multicustomer environments. For example, an application might not have initially been expected to support multi-factor authentication or its database designed to partition data by tenant.

Dashboards	Reports
n/a	Vulnerabilities on Shared Technologies

Vulnerabilities on Shared Technologies
    Lists the vulnerable technologies that a malicious user might exploit.

Understanding the Foundation Dashboards and Reports

Available only with ArcSight capabilities.

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

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

Category	Dashboards	Reports
Entity Monitoring	Account Management Login Activity Overview	All Logins by Hostname Failed Logins Summary Login Activity by User
Events Overview	Least Common Events Most Common Events Most Common Events by Severity Reporting Devices	n/a
Hosts Monitoring	Host Profile Overview	Anti-Virus Activity Anti-Virus Stopped or Paused Audit Log Cleared Failed Anti-Virus Updates Summary Operating Systems Errors and Warnings Services Shutdown Services Started

Category	Dashboards	Reports
Malware Monitoring	Attacks and Suspicious Activity Overview Malware Overview Web Application Attacks	Reported Malware by Host Worm Infected Systems
Network Monitoring	DGA Overview DoS Activity Email Attacks IDS Events Overview Man in the Middle Attacks Reconnaissance Activity SSH Attacks Traffic Anomaly Overview VPN Activities Overview	Exploit Attempts Detected by IDS Network Device Configuration Changes
Perimeter Monitoring	Firewall Blocked Events Firewall Traffic Overview	Firewall Configuration Changes Firewall Blocked Traffic by Destination Address
Vulnerability Monitoring	Vulnerability Overview	High Risk Vulnerabilities by Host SSL Vulnerabilities Vulnerability Overview Vulnerabilities by Host XSRF Vulnerabilities XSS Vulnerabilities

Entity Monitoring

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:

Dashboards	Reports
Account Management	All Logins by Hostname
Login Activity Overview	Failed Logins Summary
User Profile Overview	Login Activity by User

Account Management

Provides charts and a table to view actions associated with account management.

Charts:

- Source User, Modification, Outcome, and Account
- Account Management Actions
- Account Modification by User
- Timeline

Special Views

- Accounts by Action Type
- Management Account Distribution
- Windows Account Privilege Change

Filters

- Device Vendor and Product
- Outcome
- Action Type

Login Activity Overview

Provides an overview of login activity. The table shows the details of the event, and if you click **Global Event Id**, it will take you to the **Event Inspector**. You can also click **Open Search** and it will take you to the search page and loads the `categoryBehavior = /Authentication/Verify` query with the same time that the dashboard was run.

Charts:

- By Destination User
- By Destination Host
- By Source Address
- Timeline

Special Filters:

- Login Activity Distribution

- Windows Logon Type

Filters:

- Login Outcomes

- Device Vendor and Product

User Profile

Displays information about a specific user's actions in your environment. This is a drill-down dashboard that can be opened with a specific user from another dashboard, table, bar, chart, or entered in the dashboard search bar. The dashboard requires a valid user to show information.

Charts:

- Log In Connections

- Account Management Actions

- Traffic by Volume

- Requested URLs

- Processes Used

- Application Protocols

- Timeline

Filters:

- Device Vendor and Product

- Category Outcome

- Category Significance

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 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.

Events Overview

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:

Dashboards	Reports
Least Common Events Most Common Events Most Common Events by Severity Reporting Devices	n/a

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

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:

Dashboards	Reports
Host Profile Overview	Anti-virus Activity
	Anti-virus Stopped or Paused
	Audit Log Cleared Events
	Failed Anti-virus Updates Summary
	Operating System Errors and Warnings
	Services Shutdown
	Services Started

Host Profile Overview

Displays the activity on a specific host. This is a drill-down dashboard that can be opened from IP addresses or host names located in a table, bar, chart, or entered in the dashboard search bar. The dashboard requires a valid IP address or host name to show information.

Charts:

- Inbound Connections
- Outbound Connections
- Source Users Associated
- Destination Users Associated
- Timeline

Filters:

- Device Vendor, Product, and Class ID
- Category Outcome
- Category Technique
- Application Protocol

Anti-virus Activity

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

Anti-virus Stopped or Paused

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

Audit Log Cleared

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

Failed Anti-virus Updates Summary

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

Operating Systems Errors and Warnings

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

Services Shutdown

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

Services Started

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

Malware Monitoring

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 unusual activity that affects hosts, use the following reports:

Dashboards	Reports
Attack and Suspicious Activity Overview	Reported Malware by Host
Malware Overview	Worm Infected Systems
Web Application Attacks	

Attacks and Suspicious Activity Overview

Displays an overall view of new threats and monitor your devices.

Charts:

- Suspicious Activity Relationship

- Attack/Target Matrix

- Timeline

- Top 5 Ports

- SSH Attacks- drilldown to SSH Attacks Overview Dashboard

- Web Attacks- drilldown to Web Attacks Overview Dashboard

Filters:
- Agent Severity

- Attack Technique

Malware Overview

Displays the number of malware events, malware detected in your environment, and the infected hosts.

Charts:
- Top Reported Malware

- Malware Distribution

- Infected Assets

- Outcome, Action, and Malware

- Timeline

Filters:
- Device Vendor and Product

- Login Outcome

- Severity

Web Application Attacks

Displays information from web-based attacks on your environment.

Charts:
- **Type of Web Application Attack**

- **Targeted Host**

- **Attacker IPs**

- **Timeline**

Filters:

- Device Vendor and Device Product

- Category Techniques

- Agent Severity

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

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-inthe-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:

Dashboards	Reports
DGA Overview	Exploit Attempts Detected by IDS
DoS Activity	
Email Attacks	Network Device Configuration Changes
IDS Events Overview	
Man in the Middle Attacks	
Reconnaissance Activity	
SSH Attacks	
Traffic Anomaly Overview	
VPN Activities Overview	

DGA Overview

Helps you watch for domain generation algorithms (DGAs). DGAs make it easier for adversaries to introduce malware to your environment.

Charts:

- Affected IPs

- Suspicious Domains Generated

- Affected IPs by Bytes Out

- DGA Activity Relationship

- Timeline

Filters:

- Affected IP

- Suspicious IP

- DGA Domains

- Query Type

DoS Activity

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

This dashboard also is available in the Denial of Service category of the Cloud reports.

Email Attacks

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

Exploit Attempts Detected by IDS

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

IDS Events Overview

Helps you identify events generated by Intrusion Detection Systems.

Charts:

- Attacker IPs

- Targeted IPs

- Distribution by Category Technique

- Timeline

Filters:

- Device Vendor, Product, and Signature ID

- IDS Type

- Category Technique

Man in the Middle Attacks

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

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

Network Device Configuration Changes

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

Reconnaissance Activity

Helps you watch for reconnaissance activity, which occurs when attackers are collecting information about your system in order to find vulnerabilities for future attacks.

Charts:

- Reconnaissance Events

- Targeted Users

- Targeted IPs

- Target Ports

- Category Technique

- Source IPs

- Timeline

Special Views:

- *Source IP-Target IP Relationships* serves as a scatter chart showing the relationship between source and target IPs.

- *Reconnaissance Activity Distribution* provides a distribution map displaying reconnaissance activity.

Filters:

- Device Vendor and Device Product

- Targeted Users

- Transport Protocol

- Category Technique

- Agent Severity

Traffic Anomaly Overview

Helps you identify anomalies in network traffic.

Charts:

- Anomalies Detected

- Targeted Ports

- Source IPs

- Targeted IPs

- Timeline

Special Views:

- *Source IP- Target IP Relationship* which provides a scatter chart displaying the relationship between source and target IPs.

- *Traffic Anomaly Distribution* which provides a distribution map displaying traffic anomalies.

- *Traffic by Volume*, which provides a line chart displaying traffic volume over time.

Filters:

- Device Vendors and Products

- Anomaly Type

- Application Protocol

- Transport Protocol

- Category Significance

SSH Attacks

Displays an overview of SSH protocol usage so that you can monitor threats and see vulnerabilities in your environment.

Charts

- Type of SSH Attacks

- Top Targeted Users

- Top Targeted IPs

- SSH Activity Relationship

- Timeline

Filters:

- Device Vendor, Product, and Class ID

- Source User

- Category Technique

- Category Significance

- Agent Severity

> **Note:** The Timeline chart for the SSH Attacks Activity Overview populates using baseEventCount received from the connectors.

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

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

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

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

Dashboards	Reports
Firewall Blocked Events	Firewall Configuration Changes
Firewall Traffic Overview	Firewall Blocked Traffic by Destination Address

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

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

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

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

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

Dashboards	Reports
Vulnerability Overview	High Risk Vulnerabilities by Host
	SSL Vulnerabilities
	Vulnerabilities by Host
	XSRF Vulnerabilities
	XSS Vulnerabilities

Vulnerability Overview

Provides information to help you track vulnerabilities reported in your enterprise.

Charts:

- Vulnerabilities Detected

- Vulnerable Hosts

- Agent Severity

- Timeline

Filters:

- Device Vendor, Product, and Signature ID

- Agent Severity

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.

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.

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®. 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 webbased 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
Cryptographic Failure	Information Leaks Overview	Organizational Records Information Leaks Personal Information Leaks
Identification and Authentication Failures	N/A	Broken Authentication and Session Management
Injections	Injection Vulnerabilities Overview XSS Vulnerabilities	Command Injections on HTTP Request Cross Site Scripting Injection Vulnerabilities SQL Injection
Software and Data Integrity Failures	Deserialization Flaws Overview	Deserialization Flaws
Security Logging and Monitoring Failures	Attacks and Suspicious Activity Overview Failed Logins Overview Login Activty Overview Security Log is Full	All Logins by Hostname Audit Log Cleared Failed Logins Summary Operating System Errors and Warnings
Security Misconfiguration	Misconfiguration Events Overview Missing Security Patches Overview XML Vulnerabilities Overview	Security Patch Missing XML Vulnerabilities
Server-Side Request Forgery	N/A	Server-Side Request Forgery
Vulnerable and Outdated Components	SSH Vulnerabilities Overview Vulnerability Overview	SSH Vulnerabilities Summary SSL Vulnerabilities

Broken Access Control

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 1 - 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.

Dashboards	Reports
n/a	Broken Access Control

Broken Access Control
    Lists vulnerable hosts by severity over time.

Cryptographic Failures

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 2 - Cryptographic Failures**.

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.

Dashboards	Reports
Information Leaks Overview	Organizational Records Information Leaks
	Personal Information Leaks

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.

Injections

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 3 - 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.

Dashboards	Reports
Injection Vulnerabilities Overview	Command Injections on HTTP Request
XSS Vulnerabilities	Cross Site Scripting
	Injection Vulnerabilities
	SQL Injection

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.

Cross Site Scripting

Lists events associated with XSS vulnerabilities.

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.

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

XSS Vulnerabilities

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

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

Security Misconfiguration

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 5 - Security Misconfiguration**.

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

Dashboards	Reports
Misconfiguration Events Overview	Security Patch Missing
Missing Security Patches Overview	XML Vulnerabilities
XML Vulnerabilities Overview	

Misconfiguration Events Overview

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

Missing Security Patches Overview

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

Security Patch Missing

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

Older or mis-configured 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.

XML Vulnerabilities
Lists the hosts with the most XML vulnerabilites.

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 vulnerabilites. You can review the vulnerabilities by severity and risk indicator.

Vulnerable and Outdated Components

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 6 - Vulnerable and Outdated Components**.

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.

Dashboards	Reports
SSH Vulnerabilities Overview	SSH Vulnerabilities Summary
Vulnerability Overview	SSL Vulnerabilities

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

SSH Vulnerabilities Summary
Lists the hosts reported to have the most SSH vulnerabilities.

SSL Vulnerabilities
Lists the hosts reported to have the most SSL vulnerabilities.
This report also is available in the Vulnerability Monitoring category of the **Foundation** reports.

Vulnerability Overview

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

Identification and Authentication Failures

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 7 - Identification and Authentication Failures**.

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

Dashboards	Reports
n/a	Broken Authentication and Session Management

Broken Authentication and Session Management
Reports the top 20 hosts with the most reports of broken authentication and system management. The table lists the IP address, host name, ID of the device event class, and the number of reported events. This report also is available in the Account Hijacking category of the **Cloud** reports.

Software and Data Integrity Failures

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 8 - Software and Data Integrity Failures**.

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.

Dashboards	Reports
Deserialization Flaws Overview	Deserialization Flaws

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.

Security Logging and Monitoring Failures

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 9 - Security Logging and Monitoring Failures**.

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:

Dashboards	Reports
Attacks and Suspicious Activity Overeiew	All Logins by Hostname
Failed Logins Overview	Audit Log Cleared
Login Activity Overview	Failed Logins Summary
Security Log is Full	Operating System Errors and Warnings

All Logins by Hostname

   Lists all logins that have occurred on the specified host.

Attacks and Suspicious Activity Overview

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

Audit Log Cleared

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

Failed Logins Overview

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

Failed Logins Summary

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

Login Activity Overview

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

Operating System Errors and Warnings
Provides charts and a table that report the operating systems errors and warnings in the organization.

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

Server-Side Request Forgery

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 10 - Server-Side Request Forgery**.

When server-side web applications fetch remote resources without checking the user-supplied URL, attackers may force the application to send a crafted request to an unexpected destination including those protected by a firewall or VPN.

Dashboards	Reports
n/a	Server-Side Request Forgery

Server-Side Request Forgery
Lists any Server-Side Request Forgery (SSRF) events that occur in your environment. This report provides details including: relevant hostnames, event IDs captured, the product that captured the events, and the number of times the event occurred. Additionally, this report has a chart for a visual representation of the information.

Responding to Threats

Select **RESPOND**.

ArcSight SOAR helps you respond quickly to threat detection and remediation by providing multiple forms of automation, analyst augmentation, collaborative investigation and response. With SOAR fully integrated in the Fusion capability, the system listens to alerts, forwarded from different components to identify a threat possibility. For Fusion to receive an alert, you must ensure that SOAR is integrated with other components such as the Real-time Threat Detection service available in ArcSight SIEM as a Service (SaaS).

Introduction to SOAR

Security **O**rchestration **A**utomation and **R**esponse platform combines orchestration of technology and people, and automation and case management into a seamless experience. By providing tactical automation and orchestration through a single pane of glass, it enables SecOps teams to ramp up their output despite a growing cybersecurity skills gap and an increasing volume of complex attacks and alerts.

Overview of SOAR

ArcSight SOAR delivers an automated case response solution for repetitive security events and imparts a seamless security management experience by performing faster threat detection and remediation.

The main value proposition of SOAR lies in assisting your organization for human and machine-led analysis of the alerts, and leveraging an automated solution for threat response and remediation.

SOAR is fully programmable and can easily integrate with the existing technology stack of your organization. This application is capable to meet security teams' unique needs, and enables multiple forms of automation, analyst augmentation, collaborative investigation and response through an intuitive interface.

SOAR Features

Some of the key features of SOAR includes:

Case Management: SOAR enables you to manage and collaborate data to resolve case efficiently on a single pane of glass. The case management helps streamline investigations and expedite case resolution.

Consolidation: You can aggregate alerts from different sources based on configured time-span or common conditions. This helps in gathering all the correlated information for the suspected threat and further helps in finding the optimized solution for case handling.

Orchestration: The automated solutions provided by SOAR can seek information from the SOC or pass the control to the security operations center (SOC) for decision making and then take the control back to automation. Depending on the case scenario, ArcSight SOAR can orchestrate the control flow from automation to human analyst.

Enrichment: The system uses enrichment feature to gather additional information about the event contexts. These additional insights act as guides to carry on the detailed threat investigation.

Automation: The system leverages both fully automatic and semi-automatic solutions for threat remediation and response. You can automate mundane repetitive tasks, prioritize events and streamlines security processes to deliver accelerated case response.

Response: SOAR automation can execute protective actions, stored in playbooks, to prevent any threat impact to your organization. This capability offers unique solution to respond to events in a quick and effective manner.

Reporting and Analytics: You can generate reports to view detailed information about cases. SOAR offers a pre-defined report template for data presentation or you can create your own template to specify which data you want to include. To analyze the data further, you can view all data statistics in the form of tables and charts in Dashboard.

Challenges Faced by Organizations:

Existing cybersecurity landscape presents lots of challenges to the organizations including:

- **Attack speed**: Attacks keep getting faster every day. Modern attacks are almost entirely automated.

- **Attack volume**: An average organization gets more than 300 cyber alerts per day (IDC). Investigating and responding to an alert takes around 8 full hours.

- **Disparate tools**: SOC analysts use 15- 20 different tools throughout their daily jobs to investigate and respond to attack alerts. Tier-1 analysts are not able to investigate (and use the tools) and they are merely expensive human filters.

- **No single pane of glass**: There is no trail of investigation and response activities and there isn't a proper answer to "who is working on which case and doing what" at any point in time on the SOC floor.

- **Lack of KPIs and metrics**: As most SOCs lack the practice of investigation and response, it is almost impossible to come up with relevant, easy-to-collect KPIs and metrics. Getting a grip on who needs more training, SLA adherence, case backlog trends, etc. is difficult and intuitive-only.

- **Cyber Security Skill Shortage**: Currently, the cybersecurity sector is facing a severe expert shortage. Currently, there are 350,000 vacant positions in the U.S. alone and the industry shortfall is expected to rise to 3.5 million cyber expert vacancies.

Understanding SOAR Workflow

SOAR receives alerts from different sources. These alerts are processed to form cases. The newly created case are dispatched to SOCs. Most of the cases can be resolved automatically by executing associated playbooks, however, at times human interventions are needed for decision making.

Following figure presents a general workflow of ArcSight SOAR:
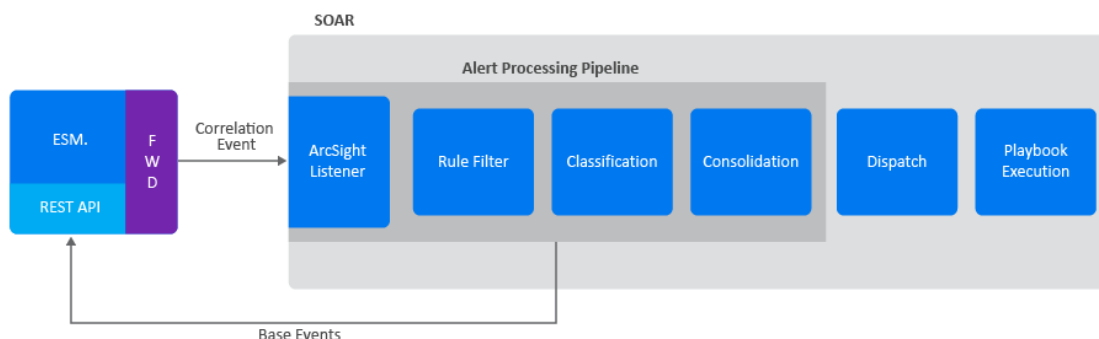
1. ESM Sending Alerts to SOAR

2. Processing Alerts

   a. Receiving Alerts Through ArcSight Listeners

   b. Defining Action Plans by Rule Names

   c. Classifying Alerts

   d. Consolidating Alerts to form cases

3. Dispatching cases

4. Automating case Handling by Playbooks

ESM Sending Alerts to SOAR

The ArcSight ESM forwards alerts and their respective correlated events to SOAR to identify, analyze and resolve a probable attack. To send alerts to SOAR, ESM must be integrated and configured as an alert source on the SOAR platform. SOAR receives alerts with rule names that were defined at the ESM. The rule names are used for alert classifications during case creation.

When an alert is created, the ArcSght ESM stores various base events that produced that alert. For example, if a **Remote Port Scan Detected** alert is created, the ESM will store a number of events, each with a separate log entry received from systems under attack or probe. SOAR gets these base events since they contain useful information (for example time of each event, attacker username and attacker remote address) through correlated events. These information are displayed on the case page, created and bound with the respective alert. The correlated events are also helpful during defining the scope items for the alert analysis.

Processing Alerts

After integrating with ESM, SOAR follows a set of procedures for alerts processing as follows:

Receiving Alerts through ArcSight Listener

After configuring ESM as an alert source, the ArcSight Listeners starts listening to the configured ports and get alert messages. These alert messages are usually brief including useful information, for example the type of alert, time of event, count of base events that produced the alert, and the severity of the alert. Context of the alert messages depends on the alert source and the rules configured.

Defining Action Plans by Rule Names

A rule name is configured as pre-processor rules in the ESM for tagging and forwarding the base events to SOAR. These rule decides the action plans for the alerts. Based on the directions imposed by rules an alert can be considered as a threat alert or a normal event.

Classifying Alerts

Depending upon the conditions directed by rules, a label is added to the alerts. The labeling helps in selecting the appropriate playbook/s for the case handling and response.

Consolidating Alerts to form cases

Depending upon the configuration settings, different correlated alerts are consolidated to form cases. At this point, the ArcSight SOAR decides to consolidate alerts to form a new case or the respective alert can be added to a pre-existing case.

Dispatching cases

When a new case is created, a case severity is assigned to the case, based on the severity mapping of the alert source. After the severity assignment, the case is assigned to a user or a user group. The dispatching of the case is done by running **case Dispatch Playbook**. If the playbooks cannot find an assignee, SOAR leaves the case as unassigned. Running these playbooks may find more than one assignee, but SOAR only selects the first one.

Dispatch playbooks might also change case's severity or add watchers or labels to the case.

Automating case Handling by Playbooks

After a case is created and dispatched, SOAR runs a playbook/s with matching conditions as defined during alert consolidation. All matching playbooks are executed sequentially and in their rank order. Higher rank playbooks are executed earlier.

Each executed playbook can run a number of enrichment operations and queue actions in an arbitrary order. Enrichments are synchronous, that is, playbook execution waits for their completion before continuing with the next operation.

Actions are always asynchronous. There is a separate queue of actions, manageable in the **Action and Rollback Queue** tab. Completed actions are moved from the queue to the **Alerts** tab of **Status** menu.

A completed action can be either automatically or manually rolled back, if the action's capability supports rollback operation.

If playbook contains a case close element, SOAR automatically closes the case, otherwise, case remains open after all the tasks are completed.

Setting Up SOAR

You can customize SOAR response to suit your organizational requirements.

Setting Up SOAR to Receive Alerts

Select **RESPOND** > **Configuration**.

To ensure seamless security resilience, you must configure SOAR solution to receive alerts from disparate security tools and platforms.

You must create a user credential in the **Credential** tab to communicate with other components. After a credential is created, you must add the alert source in the SOAR platform. Every alert in SOAR is generated through a rule in the alert source and whenever an alert is received by SOAR, it is received with the rules that were used to process the alerts.

After the Alert source is added, you must integrate the component with SOAR in the **Integration** tab.

You can enable additional configuration parameters for enrichment or to forward events by other component on a specific port number or any other configuration in the **Parameters** tab.

Creating User Credentials for Integration

Select **RESPOND > Configuration > Credential**.

Platform listens to alerts, forwarded from different components to identify a threat possibility. For the system to receive an alert, you must ensure that SOAR is integrated with other components. The **Credentials** tab allows you to create user credentials to interact with other components during the integration procedure.

The Credentials tab displays a list of user credentials. You can view the credential names, the last modification date and the name of the modifier.

- Searching a Credential
- Creating a User Credential
- Editing and Deleting a User Credential

Searching a Credential

You can search a specific user credential, through the **Search** option. Click the ⚙️▾ button next to search, allows you to view search results based on **ID, Credential Name** and **Last Modified By**.

Creating a User Credential

Click the **+Create Credential** button to create a new user credential. In the **Credential Editor** window, specify the details for following fields:

Type
Select <Internal Credential, External Condition>.
Internal Credentials are stored in SOAR's database table. External Credentials are stored in integrations, such as Cyberark Central Credential Provider.

Name
Specify a name for the credential set.
The name that you create here is displayed in the Credentials field during alert source and integration configuration. You must select this name to ensure that SOAR communicates with other components through this name identity.

Username
Specify a username for the credential set.

Password
Specify a password for the credential set.

Private Key
Specify a private key for the credential set, if needed.

Editing and Deleting a User Credential

To edit an existing user credential, complete the following steps:

1. Click **Edit** in the **Actions** column.

2. In the **Credential Editor** window, specify the values as per your requirement.

3. Click **Save**.

4. (Optional) To delete an existing credential, click **Delete**.

> You cannot delete a user credential that is used in the integration with other components.

Configuring an Alert Source

Select **RESPOND > Configuration > Alert Source**.

To ensure seamless reception of the correlated alerts, you must configure an alert source. The **Alert Source** tab allows you to create new alert source configurations, displays a list of existing alert source configuration and options to modify the existing alert source configuration.

- Creating an Alert Source Configuration
- Editing and Deleting an Alert Source Configuration
- Configuring SOAR as an Alert Source

Creating an Alert Source Configuration

Click **+ Create Alert Source Configuration** button to create a new alert source configuration. In the **Alert Source ConfigurationEditor** window, specify the details for following fields:

> You might see differences in the fields of this editor for some of the alert source types (as you select it from the Type combo box list).

Name
Represents the name of the alert source.

Type
Represents the type of the alert source. It could be one of the alert source types.

Address
Represents the IP address of the alert source to which SOAR connects when it wants to get data.

Key
Represents a unique, auto-generated key that is used as a shared token to make sure the remote IP addresses ("Allowed IP addresses") are correct. The value of this field must be included in the messages coming from those remote IP addresses.

Allowed IP addresses
Indicates that any alert coming from the specified IP addresses will be processed and others will be discarded. For most alert source types, SOAR opens a TCP port (or a web service API endpoint) and waits for some alert sources to connect. This field along with the "Key" field is to improve your system's security. The combination of these two fields prevents a potential attacker from feeding your system with fake events and causing damages.

Alert Severity
Represents the severity of alert sources. Define the severities according to the priorities of tickets produced by the alert source. Use the **Add** button to create each severity. While adding the severities, you can specify the default severity by selecting the checkbox under the **Default** column.

Configuration Content
Indicates the default configuration definitions for some type of alert sources, such as IBM Security QRadar but it is not required for many alert sources. It depends on which alert source you are trying to interact with. If there are some required data for the alert source configuration, this area shows a template and ask you to edit it if needed.

Credential
Represents the credentials defined on the system to be used for the alert source.

Show alert parameters by default
Shows the default alert parameters defined for the selected device type on the system.

Trust Invalid SSL Certificates
Instructs SOAR to connect anyways to an alert source ignoring warnings for untrusted SSL certificates. You might have installed alert sources with self-signed SSL certificates, which SOAR does not trust and deny connecting by default. Therefore, if you do not select this checkbox, SOAR still gets the brief alert, but cannot get more details on the alert.

You can click **Test** to verify if the configuration is correct.

Editing and Deleting an Alert Source Configuration

You can edit an existing alert source configuration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Alert Source Configuration Editor** window is displayed. Specify the values in the window as per your requirement and click **Save** to modify.

You can delete an existing alert source configuration by clicking the **Delete** button under the **Actions** column.

For detailed information see the related *Integration Guides*.

Configuring SOAR as an Alert Source

ArcSight SOAR creates internal alerts for some cases, such as when an action is failed permanently or an integration becomes unavailable because its firewall is not reachable. These internal alerts are generated for the event types including : action and rollback failures, auto-enrichment failures, when an integration becomes offline/online, breach of ticket resolution/first response SLAs, and custom/arbitrary alerts created by playbooks.

Integrating SOAR with Other Components

Select **RESPOND > Configuration > Integrations**.

You can configure SOAR to integrate with other platforms and components to receive alerts. This procedure ensures streamlining the alert inflow and powers automation. The **Integrations** tab allows you to create, manage and configure security integrations and platforms. The Integrations page lists integrations configured previously along with their action and rollback queue sizes, and their availability statuses.

- Searching an Integration
- Creating an Integration
- Editing and Deleting an Integration
- Testing Integration
- Flushing Queues

Searching an Integration

You can search a specific integration, through the **Search** option. Click the button next to search, to view search results based on **ID, Name, Type, Address, Availability, Last Modified By, Modification Date, Action Queue Size, Rollback Queue Size** and **Actions** filters.

Creating an Integration

Click the **Create Integration** button to create an integration. In the **Integration Editor** window, specify the details for following fields:

Name
   Name of the integration.

Type
   Type of the integration.

IP Address
   IP address of the integration.

Configuration
   Depending on the integration type, you might select and enter various configuration commands on the black window. See the below Changing Integration Configuration section for details.

Credential
   Credentials to be used to connect this integration. Credentials are defined in Credentials menu.

Trust Invalid SSL Certificates

Determines whether SOAR connects to an integration and ignores warnings for untrusted SSL certificates.

Require Approval Form

Identifies the users that need to approve action items before executing it for integrations.

Notify

Identifies the users that will be notified of actions done.

Tags

Used to group integrations. This allows creating actions on a number of integrations having the same tag. You might want to create an action for all integrations that have a specified tag such as "block offender IP address on all firewalls that are used to manage WiFi networks".

You might prefer to specify some more parameters for some specific integrations. Select the **Show Additional Parameters** checkbox located at the very bottom of the **Integration Editor** to the additional configuration.

Maintenance

Maintenance is supported by all integrations to which SOAR connects using the SSH protocol. It is essentially a generic SSH integration action script. It is best used in conjunction with Check Point Firewall integration for activating or installing a previously saved but not activated firewall policy. You can select a maintenance frequency or type your own cron job (for a scheduled maintenance) by selecting the **Custom Cron Value** option in the combobox.

Host Key

SSH public key of the remote integration. It is only used for integrations connected with SSH. If an SSH key is provided, then it will be validated using the specified key. This check is required to prevent man-in-the-middle attacks.

Batch Size

SOAR can send multiple action queue items to the integrations in a single connection. This field specifies the maximum number of action queue items that will be sent in each execution. For example, if you provided **Batch Size** as **10** and there are 25 action queue items waiting for that integration, then SOAR will send these items in 3 separate execution (10 + 10 + 5). Its default value is 1. This is a feature to avoid causing excessive system load on remote integrations when executing actions. A bigger batch size might create overhead on the integration thus failing all entries. So, you need to be careful when increasing this value.

Max Postpone

Specifies the maximum number of action retries. If an action cannot be executed for any reason, such as connection failures, authentication problems or another SOAR internal problem, it will automatically be retried later. There are a number of global configuration parameters to configure how and when it will retry, but, after a number of retries specified in this field, SOAR will give up and mark the action as failed. Default value is 6 (in hours).

Connection Limit
Specifies the maximum number of concurrent connections for the integration. Default value is 5.

Max Action Retry
Specifies the maximum action retry count for the integration. Default value is 5

Max Rollback Retry
Specifies the maximum rollback retry count for the integration. Default value is 5.

Editing and Deleting an Integration

You can edit an existing integration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Integration Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing integration by clicking the **Delete** button under the **Actions** column.

For detailed information see the related Integration Guides.

Testing Integration

Click **Test** to verify the integration configuration.

When you click the **Test** button, it triggers the availability check for integration and if anything fails, a detailed error message is displayed. For example, in the case of a Check Point Firewall integration, SOAR needs a credential to work with the integration. If a credential is not available, an error message is displayed.

If the administrator of the remote integration accidentally deletes the credential that SOAR uses, SOAR will no longer be able to create actions on the integration. In this case, the integration is shown as offline (and an internal alert is created) and the error message is logged into the error log.

You can click **Test** button to see the error message.

A successful test marks the integration as **online**.

Flushing Queues

To flush the ques, select **Flush Queue** button under the **Actions** column of the integrations list. Following is the basic flow in SOAR:

1. Alert is received.

2. Matched playbooks run.

3. Action and rollback queue objects are created (waiting for execution in the queue).

4. Actions/rollbacks in the action/rollback queues are executed and saved.

When you click the **Flush Queue** button, SOAR starts executing actions/rollbacks without waiting for the execution scheduler (which consumes action/rollback queue objects).

Configuring Additional Parameters

Select **RESPOND > Configuration > Parameters**.

You might require performing some additional configuration, depending on the component or platform integration requirements. The **Parameters** tab displays a list of parameter that can be used for the additional configuration. For more information about additional configuration for integrations, see the respective Integration Guides.

- Searching a Parameter
- Editing a Parameter

Searching a Parameter

You can search a specific parameter, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on the following attributes:

- Parameter Name
- Parameter Value
- Default Value
- Description
- Last Modified By
- Modification Date
- Actions

Editing a Parameter

You can edit an existing parameter by clicking the **Edit** button under the **Actions** column. In the **Configuration Editor** window, specify the details for the following fields:

Parameter: Specify the parameter name.

Value: Specify the parameter value.

Description: Specify the parameter description.

Default Value: Specify the default value of the parameter.

> You can not delete a parameter as it can be used in several integrations.

Configuring Case States

Select **RESPOND > Configuration > Cases**.

Platform enables you to customize case states such as statuses, severities, types and labels as per your requirement. You can configure multiple options to define case states to suit your requirement.

When you click the **Cases** page, you can view the following sub tabs:

- Statuses
- Severities
- Types
- Labels

Configuring Case Statuses

Select **RESPOND** > **Configuration** > **Cases** > **Statuses**.

You can configure the status options for a case. For example, you can define a case status as open, if the resolution procedure is ongoing for the case or closed, if it is already resolved, depending on your requirement. To bring in more clarity to the case status, you can associate colors with each case status that you create.

When you click **Statuses** page, a list of predefined case statuses is displayed.

Searching a Case Status

You can search a specific case status, through the **Search** option. Click the ⚙️▾ button next to search, to view search results based on **Name, Global, Open, Close, Color** and **Actions** of the case status.

Creating a Case Status

Click the **+Create Status** button to create a new case status. In the **Case Status Editor** window, specify the required details in the following fields:

Value	Description
Status Name	Name of the case status. Provide a short and explanatory name, such as, Open, Closed, InProgress.
Open Status	This allows to select whether the case will be in an open or closed state during the case progress. For example, it is in open state when the case is re-opened, or in closed state when the case is expired.
Colors	Select the color for the status from the suggested color options.

Editing and Deleting a Case Status

You can modify an existing case status by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Status Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case status by clicking the **Delete** button under the **Actions** column.

Configuring Case Severities

Select **RESPOND** > **Configuration** > **Cases** > **Severities**.

You can create your own case severity categories to suit your requirements. You can also set ranks to these severity categories as per the case handling priority.

When you click **Severities** page, a list of case severity is displayed.

Searching a Case Severity

You can search a specific case severity, through the **Search** option. Click the ⚙️ button next to search, to view search results based on **Name, Response Time, Resolution Time, Color, Rank** and **Actions** filters of the case severity.

Creating a Case Severity

Click the **+Create Severity** button to create a new case severity. In the **Severity Editor** window, specify the required details in the following fields:

Value	Description
Name	Name of the case severity.
Color	Select a color from the color palette.
Response/Resolution Time	These fields are optional and they provide what should be the response and resolution periods for a case of a specific severity. For example, for the cases of severity **Critical**, you might require shorter times for response and resolution.

When you select the **Show Additional Parameters** checkbox, following additional fields are displayed:

Parameter	Description
Resolution breach alert frequency time units	It is the frequency of notifications which are sent after the resolution of the cases of this severity has passed the **Resolution Time**.
Response breach alert frequency time units	It is the frequency of notifications which are sent after the response time for cases of this severity has passed the **Response Time**.
Response Near Time	It is the time left for Response SLA time at which SOAR sends a notification.
Resolution Near Time	It is the time left for Resolution SLA time at which SOAR sends a notification.

Editing the Rank of a Case Severity

You can reassign rank to the allotted severity. Click **Edit Rank** under **Actions** column and set the rank for the severity in the **Rank** column.

Editing and Deleting a Case Severity

You can modify an existing case severity by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Severity Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case severity by clicking the **Delete** button under the **Actions** column.

Configuring Case Types

Select **RESPOND** > **Configuration** > **Cases** > **Types**.

You can assign case types to specific types of cases with special backgrounds. Typically, a case type is assigned when the case goes through the playbooks. Depending on the playbook outcome, a case is categorized into a specific type. If no manual operation is needed for a case (as decided by the playbooks), it is assigned case as its type.

- [Searching a Case Type](#)

- [Creating a Case Type](#)

- [Editing a Case Type](#)

Searching a Case Type

You can search a specific case type, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Visible Name, Definition, Severities, Statuses** and **Actions** filters of case type.

Creating a Case Type

Click the **+Create Case Type** button to create a new case severity. In the **Case Type Editor** window, specify the required details in the following fields:

Value	Description
Name	
Definition	Explanation of the case type, e.g., for which cases this type can be used.
Visible Name	Provide a name for this case type to be shown when selecting a case type on the other pages of SOAR.
Severities	Select possible severities for this type.
Default Severity	When a case is opened by SOAR and related playbooks are executed, the default severity is assigned to the case.
Statuses	Select possible statuses for this type.
Default Open Status	Specify the default open status. When a case is opened by SOAR and related playbooks are executed, the default status is assigned to the case as open.
Default Closed Status	Specify the default closed status. When a case is closed, the default closed status is assifnws to the case.
Allow Case Reopen	Select this checkbox if you want to allow case of this type to be reopened after it is closed.
Custom Fields	Optionally, you can add your own fields to the case to be shown in the Cases page. Click the **Creat** button within the **Custom Fields** area, and type the name of field, select its type (text/date) and select whether this field will be visible, editable and shown on the Cases page when you select cases of this ticket type. After you provide the values for the fields click on the **Save** button, and your field will be added as a row within the **Custom Fields** area. You can edit or delete it using the **Edit** and **Delete** buttons, and add as many fields as you want.

Editing a Case Type

You can modify an existing case type by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Case Type Editor** window is displayed. Specify the values in the editor window as per your requirement and click **Save**.

Configuring Case Labels

Select **RESPOND** > **Configuration** > **Cases** > **Labels**.

You can mark a case with your own special tags, called label.

When you click on the **Labels** page, a list of case label is displayed.

- Searching a Case Label

- Creating a Case Label

- Editing and Deleting a Case Label

Searching a Case Label

You can search a specific case type, through the **Search** option. Click the ⚙️▾ button next to search, to view search results based on **Name, Color** and **Actions** filters of the case label.

Creating a Case Label

Click the **+Create Label** button to create a new case label. In the **Label Editor** window, specify the required details in the following fields:

Value	Description
Label Name	Specify the name of the label.
Label Color	Assign a color to the new label.

Editing and Deleting a Case Label

You can modify an existing case label by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, the **Label Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can also remove an existing case label by clicking the **Delete** button under the **Actions** column.

Setting Up User Access and Preferences

After integration and additional configuration are done, SOAR can receive the alerts from multiple components. These alerts have to be assigned to users. Each user is assigned a set of permissions in the user tabs.

Some of the case can be assigned to a group of users, so you can create user groups in the **User group** tab.

You can also create **Access Control list** to control the access of the users or user groups to SOAR objects including action capabilities, credentials, custom scripts, enrichment capabilities, enrichment plugins, integrations and integration types.

Configuring Users

Select **RESPOND > Configuration > Users**.

An admin can list and edit user roles who will be interacting with ArcSight SOAR for case handling. SOAR authenticates users from Platform's single sign on provider.

The **Users** page displays the list of users with options to modify an existing one.

- Searching for a User
- Editing a User

Searching for a User

You can search a specific user, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on user's **ID, User Name, Last Modified By, Modification Date, External User, Active User, User Role** and **Actions** filters.

Editing a User

You can modify an existing phone number and avatar by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, User Editor window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

Configuring User Groups

Select **RESPOND > Configuration > User Groups**.

The **User Group** page displays a list of user groups and provides you options to create more user group or edit an existing user group.

- Searching for a User Group
- Creating a User Group
- Editing and Deleting a User Group

Searching for a User Group

You can search for a specific user group, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on list's **Name, Content Type, Size, Action Allowed, Enrichment Allowed, Last Modified By, Modification Date** and **Actions** filters.

Creating a User Group

Click the **+ Create User Group** button to create a new user group. In the **User Group Editor** window, specify the details for following fields:

Value	Description
Name	Name of the user group. Provide an explanatory name which gives a hint about what the user group is created for.
Email	Specify an email ID for the user group.
Users	Select the users to be included in this user group.
Avatar	You can select an avatar for the group by clicking on the **Choose File** button. Any image will work. It is recommended to select image files with sizes of 200 x 200 pixels.

Editing and Deleting a User Group

You can edit an existing user group by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **User Group Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can remove an existing list by clicking the **Delete** button under the **Actions** column.

Configuring Access Control Lists

Select **RESPOND > Configuration > Access Control Lists**.

The Platform provides **Access Control Lists** (ACLs) to control the access of the users or user groups on SOAR objects. These objects include action capabilities, credentials, custom scripts, enrichment capabilities, enrichment plugins, integrations and integration types. For example, you might prefer a specific group of users to access some specific integrations. In such scenarios you can edit the access controls of the user groups in **Access Control Lists** tab.

When you click **Access Control Lists** tab, a list of SOAR objects along with users or user groups who can access those objects, and the last user and last modification date of an access control is displayed.

- Searching an Access Control List
- Editing and Resetting an Access Control List

Searching an Access Control List

You can search a specific access control list, through the **Search** option. The search list keeps getting updated as you type. Click the button next to **Search**, to view search results based on **Object, Access, Last Modified By** filters.

Editing and Resetting an Access Control List

You can edit an existing access control list by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Access Control List Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can only edit the **Allow Access For** and **Users/Groups** fields. By default, the object list is created with the **Anyone** option. If you want to narrow down the users for an object, just edit the related object and specify the users or groups for the option you selected in the **Allow Access For** field, which can be **Only selected users/groups** or **Anyone except selected users/groups**.

After editing an **Access Control List** item, **Clear** button appears in the **Actions** column of that item. You can not remove an **Access Control List** item from the list. By clicking on the **Clear** button under the **Actions** column, you can reset value of the **Access** column.

Setting Up SOAR for Customization

Select **RESPOND > Configuration > Customization Library**.

You can customize case management through plugin scripts, email templates, query templates, scriptable integration codes, text and HTML templates (used for notifications and other capabilities) and other customizations. The **Customization Library** tab displays a list of customization, and also allows you to create a new customization content or modify an existing one. When a new plugin is uploaded through configuration/integrations/upload plugin options, you can also view and manage its code on this tab.

The list of customization can be filtered to display all integrations customizations, all integration types customization and all script types customization.

- Searching a Customization

- Creating a Customization

- Filtering Integration Customizations

- Filtering Integration Types Customizations

- Filtering Script Types Customizations

- Editing, Deleting and Reseting a Customization

Searching a Customization

You can search a specific user customization, through the **Search** option. Click the button next to **Search**, to view search results based on **ID, Name, Script Type, Integration Types, Integration, Last Modified By, Modification Date** and **Actions** filters.

Creating a Customization

Click the **+Create New Customization** button to create a new customization. In the **Customization Editor** window, specify customization name, description and type and enter the respective code in the black console.

Filtering Integration Customizations

Click **Show all integrations** filter to view the customization list based on the visible name of the integrations already defined on the environment.

Filtering Integration Types Customizations

The **Show all integration types** filter enables you to filter the list based on integration/plugin type.

Filtering Script Types Customizations

When you click **Show all scripts type** filter, a list of script type customizations is displayed.

Editing, Deleting and Reseting a Customization

You can edit an existing customization configuration by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Customization Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing customization configuration by clicking the **Delete** button under the **Actions** column.

The **Reset** button resets the content of customization to out-of-the-box version.

The **Lookup** button shows the details about where this particular customization is being used.

Referencing Documents

Select **RESPOND > Configuration > Document Repository**.

The system can store your reference documents that might be linked to cases if needed. For example, you can add case handling guides for your SOC analysts and link these documents automatically when a case is created on SOAR.

- Searching a Document
- Uploading a Document
- Editing and Deleting a Document From The Repository

Searching a Document

You can search a specific document, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on document's **ID, File Name, Title, Description, File Size** and **Actions** filters.

Uploading a Document

Click the **+Upload Document** button to upload a new document in the repository. In the **Document Repository Editor** window, specify details such as document **Title, Description** and then select the file to be uploaded.

Editing and Deleting a Document From The Repository

You can edit an existing document by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Document Repository Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can delete an existing document by clicking the **Delete** button under the **Actions** column.

To download a document click the **Download** button under the **Actions** column.

Storing Lists in SOAR

Select **RESPOND** > **Configuration** > **Lists**.

The system can store a diverse set of values in lists. The lists are used as lookup tables for referencing purpose.

- Searching a List
- Creating a List
- Editing, Deleting and Downloading a List

Searching a List

You can search a specific list, through the **Search** option. Click the [⚙▾] button next to search, to view search results based on list's **Name, Content Type**and **Size** filters.

Creating a List

Click the **+Create List** button to create a new list. In the **List Editor** window, specify the details of list as follows:

1. **List Name**: Specify the name of the list that you want to create. For Example, VIP user names.

2. Select the option **Add Column** to create a new list. You can select Delete Column option if you are modifying an existing list.

3. Select the type of the data for the list from the drop down menu, for example, user name.

4. Specify the name of the column and click **Add**. The column name is displayed in below pane.

5. Enter a list item in the text field below the column name and then click **Add List Item** to add the list item for the newly created column.

   > Enter the list item in JSON format.

6. (optional) Enter a list item and click **Search** for searching a list item.

7. Click [✎] button to display the console pane. Click **Expand JSON**, to view list item in a JSON formatted order on the console.

8. Under **Actions** tab, click **update** to add the list item in the list or click **discard** to remove the list item.

9. (optional) Select the **Restrict Actions** checkbox to ensure that any action can not be taken (even if the action is a part of the playbook instructions) on the list items defined in the newly created list.

10. (optional) Select the **Restrict Enrichments** checkbox to ensure that any enrichments can not be fetched (even if the fetching enrichment is a part of the playbook instructions) for the list items defined in the newly created list.

Example use case:

You might create a list to store the IP addresses of your data center. When you mark the list for **Restrict Actions** checkbox, SOAR will not take any actions for the servers listed in the list even if they are involved in a case. For example, your play book might contain a step to block all IP addresses on the Case scope, however it will not block those addresses defined in this list.

As another use case, you might define a list of VIP usernames. When you mark it for **Restrict Enrichments** checkbox, SOAR will not perform enrichments on these VIP users.

Editing, Deleting and Downloading a List

You can edit an existing list by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **List Editor** window is displayed. Specify the details as per your requirement and click **Save**.

You can delete an existing list by clicking the **Delete** button under the **Actions** column.

You can also download a list as a text file (txt) by clicking the **Download** button.

Setting Up Scope Items

Select **RESPOND > Configuration > Scope Item Property**.

With ArcSight SOAR 3.4, it is possible to create your own scope item property types and use them in your workflows. In order to define a new scope item property, click **Create Scope Item Property** button and specify the **Name** and **Data Type** fields. Scope item property can possibly be a:

- Number
- Text
- Json
- Percentage
- Boolean

Downloading Executables for SOAR

You must download the following executables that are used by the Windows Remote Management enrichment plugin:

Executables	Links to Download
Screenshot.exe	Download Screenshot.exe
PsExec.exe	Download PsExec.exe
curl.exe	Download curl.exe
procdump64.exe	Download procdump64.exe
volatility-2.5.standalone.exe	Download volatility2.5.standalone.exe
winpmem-2.1.post4.exe	Download winpmem-2.1.post4.exe

These executables must be downloaded at the at the volume path of the SOAR container. For default tenant, tools directory is located in the following path:

```
/opt/arcsight-nfs/arcsight-volume/soar/default/tools/win64
```

After downloading the executables, you must define them in the **Configuration** > **Parameter** tab of the SOAR application.

Configuring Rest Clients

Select **RESPOND** > **Configuration** > **Rest Clients**.

To integrate with SOAR, a third party application needs a set of credentials generated at SOAR application. You can create these credentials at Rest Client.

When you click on the **Rest Clients** page, a list of case label is displayed.

- Searching a Rest Client
- Creating a Rest Client
- Editing and Deleting a Rest Client

Searching a Rest Client

You can search a specific third party application integration details, through the **Search** option. Click the ⚙⏷ button next to search, to view search results based on **ID**, **Client ID**, Description, **Last Modified By,Modification Date** and **Actions**.

Creating a Rest Client

Click the **+Create Rest Client** button to create a new Rest Client. In the **Rest Client Editor** window, specify the required details in the **following** field and click **Save**.

Value	Description
Client ID	Specify the rest client ID.
Description	Specify the description of the rest client.

When you create a rest client by clicking save, a client secret is created for this rest client and displayed in the **Rest Client Details** window.

Ensure to note down the rest client secret along with the credentials as these would be needed whenever you call SOAR application using the REST API.

> **Note:**If you have lost the **Client ID** and **Client Secret** that you created for the rest client then you can not call the SOAR application using the respective REST API. In such cases, you must create the **REST Client** credentials along with the **Client Secret** again.

Editing and Deleting a Rest Client

You can modify an existing rest client by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, the **Rest Client Editor** window is displayed. Specify the description in the editor window as per your requirement and click **Save** to modify.

You can also remove an existing rest client by clicking the **Delete** button under the **Actions** column.

Working With Cases

ArcSight SOAR help you analyze numerous alerts, coming from an array of varied alert sources. Depending on the severity and other details, these alerts are then used by SOAR to generate cases. You can map these cases on the **Cases** tab and get a comprehensive, end-to-end understanding.

Understanding Cases User Interface

SOAR has a very user friendly interface for tracking, viewing and managing cases in a single pane of glass. The **Case** tab enables you to perform multiple operation on one page. You can view the list of cases, edit the case information such as its label, status and priority, add and edit assignees, add watchers , related cases, comments, and attach files, all on a single **Case** page. To perform a deeper analysis, you can also fetch enrichment for cases and perform desired actions. The Case Management service desk also facilitates the flexibility to create manual cases and generate reports for analysis.

A typical **Case** page is displayed as follows:
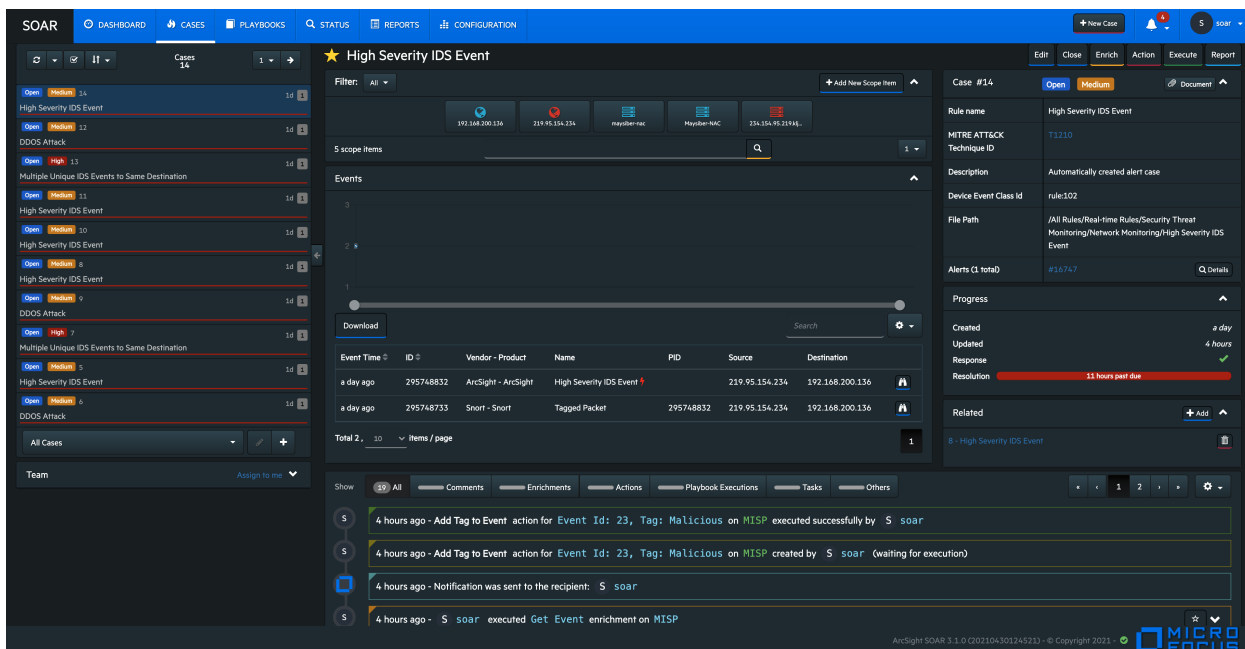
Viewing Case Details

Select **RESPOND** > **Case**.

Viewing a case workflow is very beneficial in understanding the investigation procedure and performing end to end case management. When you select a case in the case list pane, its respective details are displayed in the panes next to it, including:

- Case Name

- Scope Item Details

- Event Details

- Activity Details

- Teams

- [Case Details](#)

- [Case Progress Details](#)

Case Name

The name of case is displayed at the top. A star icon before the case name signifies that you are set as case watcher.

Scope Item Details

You can view the list of the scope item defined for the case in the scope item pane of the **Case** page. Typically, scope items are artifacts or data that supports or relates to a particular case. These can be computer name, email address, file, file name, hash, host, keyword, MAC address, network address, process, rule name, unknown, username or a URL.

To view a specific set of scope items associated with a particular case, you can filter the scope item on the basis of their source from the **Filter** button at the top of the scope item pane.

When you click a scope item, the following details are displayed:

- Name, address and type of scope item.

- Source of the scope item. Typically, a scope item can be either created by you, registered from an Alert analysis, or be imported from the files or other attachments.

- Role and Other Roles of the scope item as Impact or Offender or Related.

- Hash Algorithms used for encrypting.

- Country of origin of the scope item.

- The list of number of alerts with the same scope item.

  This alert list helps in narrowing down the investigation by understanding the malicious intent of the scope item in question. You can click the **Show alerts with this scope item** link to view the list of alerts with the same scope item. The **Alerts** list displays **Alert ID, Case, Creation Date, Rule Name and Actions** taken for resolving the related case. To view the actions and all the information captured for a particular case, click **Actions**.

Exporting/Importing STIX file

SOAR allows you to share Cyber Threat Intelligence (CTI) information over a standard based serialization format called Structured Threat Information Expression (STIX) files. This information sharing format has accelerated the effectiveness and accuracy of SOAR solutions, as the information displayed are precise enough to be picked up by the analyst or stored as machine readable JSON bundles. SOAR creates the bundle with domain

object types of indentity, indicatior, marking-definition for TLP and statement based on selected scope item.

You can export the scope items details in the STIX format to the other security applications, or import the STIX files to extract the scope items for the case analysis.

> **Note :**SOAR supports STIX format information sharing for limited scope items including network address, URL, hash, email address, user name, mac address, host name and keyword.

To export the scope items to STIX format:

1. Click **enrich** button on the top right corner of the **Case** window.

2. Enter stix in the **Launch Enrichment Plugin** window.

   The preassigned values for **Group Name**, **Enrichment Plugin**, and **Capability** fields are automatically displayed as Utilities, STIX Utilities and Export to STIX respectively.

3. Select the scope Item that you want to export in the STIX file from the **Scope Items** drop-down list.

4. Select the **Indicator Type** as applicable for the specified scope item. To know more about the scope item indicators, see STIX Indicator Type.

5. Specify the name of the STIX object in the **Name** field and add a suitable description in the **Description** field.

6. Select the appropriate **TLP Markings**. The TLP Markings are predefined specifications for standard STIX export. To understand more on TLP Markings, see STIX TLP Marking Type.

7. Mark the **Do not use cache** option as per your requirement.

8. Click the **Enrich** button. A STIX file is automatically generated and all the details of scope items can now be exported through bundled STIX file in Json format.

   Once the STIX file is generated, it gets downloaded automatically and the enrichment record is displayed in the case timelines pane at the bottom of the **Case** page.

   The STIX Json file gets its identity objects from **Customization Library**.

   You can customize the Json file fields as per your organizational details, by defining the values of the **STIXOrganizationName** parameter in the **Parameters** tab of the SOAR application user interface.

   You can modify following fields in the **STIXOrganizationName** parameter:

   ```
   {"organizationName": "Organization","sectors":
   ["defense"],"contactInfo": "contact_
   ```

```
info@organization.com","statement": "Copyright (c) Organization
2021."}
```

The values that are defined in **STIXOrganizationName** parameter is used during exporting STIX Json bundle's object of indentity type.

To import the scope items to STIX format:

1. Click **+Add New Scope Item** in the Scope Item pane.

2. In **Scope Item Form Editor** window, click **Import scope from file** button.

3. Select and open the bundled STIX file to be uploaded in the **File Upload** window.

   After opening the json bundle file, you can view the scope item name, category and the assigned role.

   > Note: If the Json file to be uploaded is not a valid STIX file, SOAR displays an error message about the invalid file format.

4. Click **Save** to extract the scope item details and add the newly fetch scope item to the case scope list.

   > Note: You can download some of the sample STIX files by clicking on **Example Files** button in the **File Upload** window.

Event Details

You can view the events that created the case and the graph of the incoming events in the **Events** pane. Typically, a case can be created by single event or by consolidation of multiple similar events based on the SOAR configuration settings.

The **Events** pane provides detailed information about the events including:

- Event Time

- Event ID

- Vendor-Product

- Name

- PID

- Source

- Destination

You can also customize the level of details displayed in the Events pane.

To customize the Events displayed on **Events** pane:

1. Click the setting icon on the top right.

2. Select the column names that you want to view in the Event details page.

3. Click **Apply**.

After selecting the case, click the binocular icon to view the extended detail for that specific event.

Activity Details

After you select a case, you can view the list of activities that were performed on the case in a detailed manner in the **Activity** pane. These information are displayed at the lower middle part of the **Case** page. The **Activity** pane presents following details:

- **All**: When clicked, this option displays all the list of activities performed on the case in a chronological order along with the User/User Role/Tier names.

- **Comments**: You can click on this option to view the list of comments added for this case. If you want to add some more case handling information, click on **Add Comment** button. You can also attach a file for to further improvise the case investigation.

- **Enrichments**: This option displays the enrichments fetched and used for resolving the case.

- **Actions**: Click on this option to view all the actions performed for this case.

- **Playbook Execution**: Click this button to display the playbook name that was executed to respond the selected case.

- **Tasks**: This option displays the current task assigned from the playbook.

- **Others**: Click on this option to view other related activities.

You can also add, edit or delete comments, or attach files using the editor at the bottom of the **Activity** area.

Teams

To view the assignee, source and watchers of the case, click the **Teams** button at the bottom left of the **Case** page.

Case Details

You can view case number, status, severity, rule name, MITRE ID, description and label in the **Case Details** pane. This pane also presents a list of attached document related to case. To access these documents, the **Document** button. You can also click the **Details** button, to view the list of alerts that were consolidated to form this event.

> You can view the **MITRE ATT&CK Technique ID**, for cases with suspected MITRE attack. SOAR receives these events from the ESM alert source and when you click **MITRE ATT&CK Technique ID**, an associated attack detail is displayed.

Case Progress Details

This pane shows the count of days/hours that has passed since the creation of and last update on the case. You can also track the SLA status of response and resolution here.

Creating New Case Manually

Select **RESPOND** > **Case** > **+New Case**.

> Your user role must have **Create Manual Case** permission to manually create a case.

There are two primary ways for SOAR to receive alerts:

Automatically from the alert sources, configured during other software integrations with SOAR.

Manually by the analyst, in the scenarios where other teams inform the operator about their Cases over calls or emails.

To create the cases manually, click **+New Case** at the top right of SOAR interface and specify the various values of different fields The following list describes the fields:

Parameter	Description
Type	Rule name for the type of manual Case type that you will select in the **Case Type** field. You can also use this field to create a new rule if it is not already defined in the **Rule Names**. When you start typing the rule name, this field lists you the defined rules in this combo box matching the entered characters. If the phrase you entered is not a match, just click on the **Create New Rule** in the combo box list to create one.
Subject	Subject for this new manual case which will be the headline of the case to be created.
Case Type	Case type to be selected from this combo box which are predefined on your SOAR system.
Custom Fields	You can provide values for the custom fields which are defined on your system for the selected case type.
Description	Description for the manual case to be created.

Parameter	Description
Time	Time and date of the manual case which you can select from the calendar in this field.
Severity	Severity of this manual case, defined on your system, which you can select from this combo box.
Add Scope Item	You can add a scope for this manual case by selecting the scope category and role, and entering the scope value.
Upload	You can attach a file (original email, a scanned document explaining the alert, etc.) to this manual case using the **Choose File** button in this field.

When the **Save** button is clicked, SOAR creates a new case and displays it.

Managing Cases

Case management is a collaborative process of streamlining case investigation and response activities to facilitate efficient remediation. When a case is registered, it is enriched with appropriate contextual information based on which, a suitable playbook is implemented to provide an effective response to the upcoming threat. Managing a case can include following tasks:

- Editing Cases

- Searching and Filtering Cases

- Sorting Cases

- Optimizing Threat Investigation through Scope Items

- Organizing Case Views Based on Layouts

- Adding Enrichments to Cases Performing Actions on Cases

- Performing Actions on Cases

- Closing Cases

- Executing Playbooks

- Analyzing Data Through Reports

- Relating Other Cases

Editing Cases

You can modify the case details to update its severity, status, label as per the different attack categories, re-assign it to new users, user groups, or tiers, add watchers and include informative descriptions.

Editing Individual Cases

When you select a case, the corresponding details appear on the right pane of case page.

To edit a case:

1. Select a case on case list to view its detail.

2. Click **Edit** and modify the following details on **Case Editor**:

   a. **Case Type**: Select the type of case.

   b. **Subject**: Specify the Subject.

   c. **Assignee**: Assign the case to selected Users or User Groups.

   d. **Watcher**: Select the watcher for the case from the displayed set of User or User Groups.

   > You can assign multiple watchers to a case.

   e. **Status**: Modify the case status as **Open** and **In Progress**.

   f. **Severity** : Set the severity of the case as **Urgent**, **Critical**, **High**, **Medium** and **Low**.

   g. **Description**: Add your comments about the case.

   h. **Label**: Select the label from the list of pre-configured labels to categorize the case.

3. Click **Save**.

Editing Multiple cases

You can also edit multiple case at the same time, through **Multiple Edit Mode**. When you click the [icon] button on the top of the case list, the case list toggles to a view where you can select multiple case using check-boxes. You can select cases not only shown in the current case list but also the ones listed in other pages using the navigation button.

The **Multiple Edit Mode** allows you to change the severity, status, label and assignees for the selected cases in one go, through the **Update All Selected Tickets** button. You can also discard your changes by clicking on **Discard** and execute the predefined playbooks for selected cases through clicking the **Run Playbooks Again** option.

If the **Multiple Edit Mode** button is clicked once, the button's background becomes blue and the **Multiple Edit Mode** page is displayed. If the **Multiple Edit Mode** button is clicked twice, the button's background becomes yellow, implying that all cases in the current navigated case list page are selected. When the button is clicked for the third time, up to a 1000 cases are selected for editing and the button's background turns red. To disable the multiple edit mode, click on the button for the fourth time.

Searching and Filtering Cases

To search a case, click the text field at the bottom of the case list. Enter the search query at the **Search** field.

To narrow down the search results, use the following set of predefined default filters below the **Search** text field:

- cases assigned to me

- cases I'm watching

- Open cases

- All cases

SOAR provides you an option to save your search queries. You can reuse the same saved search query, by selecting it from the **Saved Search Options**, below the **Default Search Options**.

To create a new search query:

1. Click the ⊞ button next to the search field. In the **Case Search Editor,** click **+Create**.

2. Click **Chose one of the following** and select the query criteria from the displayed list. Click the next **Chose one of the following** button and select a sub query criteria to further optimize your query.

3. To expand the search range, you can add another query criteria in the same search by clicking **+Create** button at the top of the **Case Search Editor** page.

    > You can keep including the query criteria in the same search by clicking **+Create** button.

4. Select the **Save** checkbox, then name the search query in the **Search Name** field.

5. You can clear your selections in the editor by using the **Clear Search** option.

6. Click **Close**. The newly created search will be added to the **Saved Search Options**.

You can also edit the saved search queries.

To edit the saved search queries:

1. Select a search query in the **Saved Search Options** and click the ✎ button next to the search field.

2. In the **Case Search Editor,** click **+Create**.

3. Click **Chose one of the following** button and select the query criteria from the displayed list. Based on the selection you made in the first **Chose one of the following** button, a set of related criteria list is displayed in the next **Chose one of the following** button. Select a sub query criteria to further optimize your query.

4. To further expand the search range, you can add another query criteria in the same search by clicking **+Create** button on the top of the **Case Search Editor** page.

> You can keep including the query criteria in the same search by clicking **+Create** button.

5. Select the **Save** checkbox, then name the search in the **Search Name** field and click **Save and Search** to save it or **Delete** to delete the saved search.

6. You can clear your selections in the editor by using the **Clear Search** or close it by clicking **Close**.

Sorting Cases

You can sort cases by their creation date, last update, severity, respond and resolution times. You can sort the case list by using the **Sorting** button located on top of the case list.

Optimizing Threat Investigation through Scope Items

When investigating a possible attack, it is important to understand the scope of the anomalous behavior. Scope items are artifacts related to the case.

SOAR enables you to create scope item to see the extracted artifacts of the case such as header information, email addresses, URLs, and attachments.

> The creation of a scope item depends on your role and the nature of the case.

To create a scope item:

1. Select a case in the case list to display a scope item pane in the middle of the case page.

2. Click **+Add New Scope Item**. In the **Scope Item Form Editor** page, enter the values for the Scope item. For some scope items, you can enter multiple values, such as IP addresses, separating each value with a newline.

3. Click **Select a category** to specify the type of the scope item.

4. Click **Select a role** to specify how the scope item is related with the case. **Impact**, **Offender** and **Related** are the options used to define the scope items relationship with the case.

5. Click **Add** to link the scope item to the respective case. The list of newly added scope items is displayed in the same page. You can also delete a scope item from the list.

6. You can also import the scope items from a CSV file. Click **Import scope from file** and in the **CSV Upload window**, click **Select the file**. Navigate and open the CSV file to

import.

7. Click **Selector** and specify the type of selector used in the CSV file. Click **Save** and then **Close** the page.

Click the newly created scope item to view its extended details and properties.

Organizing Case Views Based on Layouts

Following are the different layouts of SOAR application:

Tier 1 is the default layout in which case Context and Scope Items take the central focus.

Tier 2 layout is recommended for higher tier analysts who wants to handle deeper details of the cases. In this layout **Scope Items** and **Base Event** views take the central focus.

Adding Enrichments to Cases

For investigation of some cases, you might need more detailed information. Adding context makes correlation more productive, thus enhancing the investigation capabilities. SOAR presents enrichment feature to address this issue. You can use the desired plugin for the case using the **Enrich** button located at the top right corner of the **Cases** page.

When you press the **Enrich** button, the **Launch Enrichment Plugin** dialog appears to fetch more details about the case.

Enrichment plugins are grouped according to the information they provide. So, you need to first select a group from the **Group Name** area. Then, according to your group selection, related plugins appear under the **Enrichment Plugin** area. When you select an enrichment plugin from this area, its capabilities are listed under the **Capability** area. Each capability requires different information in this editor.

Performing Actions on Cases

You can trigger an action on a case at anytime using the **Action** button located at the top right corner of the cases page. These actions, such as sending a notification to a related person or blocking an IP address, might vary according to the case's special condition.

When you click the **Action** button, select an integration with which the defined action will be triggered.

Each capability requires a different information in this editor. For more information, see Integration Guides for the action capabilities.

After selecting the capability, you must set the rollback interval for the this action. Click **Rollback Mode** to select the rollback period and select the respective host for it by clicking on **Host**.

When you click on the **Create Action** button, the action will fall into the **Approval Requests** field of the **Cases** page, if any integration approval is configured. The action will be performed after it is approved. If no integration approval is configured, then action will be performed automatically.

Exclusion list control is performed before **Approval** request.

Closing Cases

You can close a case using the **Close** button at the top right corner of the page.

Select a **Close Status** for the case, from the following options:

- Closed

- Duplicate

- False Positive

- Resolved

You can also add a comment stating the reason. Click on the **Save and Close** button to close the case.

> You cannot close a case unless all the actions are approved and performed.

Executing Playbooks

To accelerate sending response for repetitive cases, you can have the system automatically execute Playbooks. SOAR also provides decision making liberty to the analyst to re mediate the anomalous case. In scenarios where human interventions are required, you can manually execute a playbook for the selected case. Click **Execute** on the case page and select the desired playbook in **Execute Playbook and Automation Bits** window and then click **Execute** to manually implement the playbook.

Analyzing Data Through Reports

Reporting captures the detailed analysis of the respective case including:

- Case summary

- Case timeline graphs

- Scope item recurrence analysis chart

- Detailed case timeline with actions, presented in a tabular format.

To generate a **Detailed Case Report**, click **Reports** on the case page.

Relating Other Cases

To add other cases that you want to relate with this case, click **Add** on the **Related** pane at the bottom right of the **Case** page. Specify the related case number and relation type (which could be **DUPLICATE,RELATED** and **DEPENDSON)** in the **Add New Relation** page and click **Save** to add the related cases.

> Please refer to the SOAR SMTP Integration Guide to configure email notifications.

Automating Response With Playbook

SOAR enables automated response of the repetitive cases through playbooks. The system performs actions, enrichments and/or sends tasks and notifications based on the playbooks defined in the **Playbooks** menu. You can create, modify, delete, enable or disable playbooks on the **Playbook** page.

Filtering Alerts For Case Creation

Select **RESPOND > Playbook > Rule Name Filters**.

Initially, when a Real-time Threat Detection event is received by SOAR, the rule name filters are automatically created by SOAR and must be edited as per user expectations.

At this stage, no case is formed. The rule name filters are used to decide the plan of action for an alert. The rules in this tab decide whether to register a case with the alert or not.

For example, if an alert is a possible threat, you can create a case with the alert, or you can receive the alert, save it and create a case but ignore all base events, or you can completely ignore the alert.

The **Rule Names** are listed in the ascending order in the **Rule Name Filters** page.

- Creating an Alert Source Rule Name Filter
- Managing Scope Item Extraction
- Searching for a Rule Name
- Editing an Alert Source Rule Name Filter

Creating an Alert Source Rule Name Filter

To create an Alert Source Rule Name Filter, complete the following procedure:

1. Click the **Create Alert Source Rule Name** button.

2. Specify a value for Rule Name. Make sure that the specified rule name matches with the correlation event name.

3. In the **Alert Source** menu, select an alert source from the list of created alert sources.

   For example, to add Real-time Threat Detection correlation events, select **Real-time Threat Detection** as the alert source.

4. In **Ignore Mode** menu, select one of the following values:

Parameter	Description
Create alerts	When an alert with this rule name is received, a case is created irrespective of the alert sources and alert source types. All base events will be fetched if possible.
Ignore base events	SOAR creates a case, but ignores base events if there are any
Ignore for all alert sources	SOAR does not create cases for this rule name, irrespective of alert sources defined on the system.
Ignore for all alert sources of this type	SOAR does not create a case when an alert with this rule name is received, only for the alert sources of the type shown in the **Alert Source Type** field. It creates cases for the alert sources of other types.
Ignore for this alert source	SOAR does not create a case when an alert with this rule name is received, only for the alert source shown in the **Alert Source** field. It creates cases for the other alert sources.

> **Note**: Real-Time Threat Detection Alerts are created by default with the Ignore Mode set to Ignore for all alert sources of this type. Make sure that the Ignore Mode is set to Create Alert.

5. Click **Save**.

Managing Scope Item Extraction

You cannot edit an existing *Scope Item Extraction*. You can delete an existing *Scope Item Extraction*. To delete, click **Delete** in the **Actions** column. The Scope Item Extraction Section has the following information:

Parameter	Description
Field Name	Name of the field.
Select Source	Select from the list **[Base Event, Correlated]**.

Parameter	Description
Select Category	Select from the list [**Computer Name, Email Address, File, File Name, Hash, Host, Keyword, MAC Address, Network Address, Process, Rule name, Unknown, URL, Username**].
Select A Role	Select from the list [**Impact, Offender, Related**].
Add	Click this button to add the scope item.

Searching a Rule Name

You can search a specific Rule Name. Click the ⚙▾ button next to search, which allows you to view search results based on **Rule Name ID, Rule Name, Alert Source, Ignore Mode, Pattern Matcher**, and **Actions**.

Editing an Existing Alert Source Rule Name Filter

You can modify an existing Alert Source Rule Name Filter to configure additional extraction from the base events or the correlated events.

> You cannot rename or delete an existing alert source rule name filter.

To edit an existing Alert Source Rule Name Filter, complete the following procedure:

1. Do one of the following:

   - Double-click the record that you want to edit.

   - Click **Edit** in the **Actions** column of the related record.

   For example, to edit the Alert Source Rule Name Filter for Real-time Threat Detection, make sure that the Alert Source name is Real-time Threat Detection.

2. In **Ignore Mode** menu, select a value according to your needs.

   > **Note**: Real-Time Threat Detection Alerts are created by default with the Ignore Mode set to Ignore for all alert sources of this type. Make sure that the Ignore Mode is set to Create Alert.

   You will be able to see the created tickets in the **Cases** page.

Consolidating Alerts to Create Cases

Select **RESPOND> Playbook> Consolidation**.

Multiple alerts are generated from different alert sources that are integrated with SOAR. These alerts are automatically consolidated to create a case as per the configuration settings. The **Consolidation** page displays a list of rules to consolidate alerts to create cases.

When an alert reaches the consolidation plugin based on the rules, all the correlated alerts are consolidated to create a case. It is after this consolidation procedure that the system decides whether to create a new case or to add the alert into an existing one.

Consolidation rules are processed from top to bottom and only the first match is executed. Any alerts that matches the same consolidation rule is gathered in to the same case until that case status is **Close**. In that instance, a new case will be created and alerts are consolidated into this case.

- Searching a Consolidation Filter
- Creating a Consolidation Filter
- Editing and Deleting a Consolidation Filter

Searching a Consolidation Filter

You can search a specific **Consolidation Filter**, through the **Search** option. Click the button next to search, to view search results based on **ID, Rule Conditions, Timespan, Last Modified by, Modification Date, Rank** and **Actions**.

Creating a Consolidation Filter

Click **Create Consolidation Filter** to create a new consolidation filter. In Consolidation Filter , specify the details for following fields:

Timespan: Value in minutes, hours, weeks or days. Timespan provides time intervals to consolidate alerts into one case.

Since Last Alert: Timespan will be calculated from the last alerts creation time.

Since First Alert: Timespan will be calculated from the first alerts creation time.

Until First Response: Consolidation will stop when the case is responded by an analyst. When this checkbox is selected, Platform will track the response status of the case and timespan and stop the consolidation at whichever comes first.

Create Conditions: Select a condition for alert consolidation from the following list of condition **Types** and **Parameters**:

- **Type**: Type of the consolidation. Select from the list.
    - Alert source is
    - Alert source rule name is any of

- Alert source rule name is in list

- Alert source rule name matches regex

- Scope item category is

- Scope item role is

- Scope item value does not equal

- Scope item value equals

- Scope item value is in list

- Scope item value is not in list

- **Parameters**: It varies depending on selected consolidation type.

> The newly created Consolidation Filter is displayed on the Consolidation page and is in **Disabled** state by default. You must ensure enabling the **Consolidation Filter** before using it.

Editing and Deleting a Consolidation Filter

You can edit an existing consolidation filter by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Consolidation Filter** window is displayed. Specify the values as per your requirement and click **Save**.

You can delete an existing consolidation filter by clicking the **Delete** button under the **Actions** column.

Classifying Cases on SOAR

Select **RESPOND > Playbooks > Classification**.

Classification tab helps you to organize or maintain your cases on the SOAR platform.

After an alert is received and a case is created with it, then it is passed for classification. On **Classification** tab, the alert is labeled depending upon the conditions. The rule names are checked depending on the rule name and a label is added to the alert. Later these classification labels help the system in choosing and executing a playbook for this case.

You can view a list of classification on this page. The Classification list is processed from top to bottom and only the first match is executed. You can edit the rank of a classification rule through the **Rank** option and created items will appear as the last item in the table.

- Searching a Classification

- Creating a Classification Rule

- Editing and Deleting a Classification

Searching a Classification

You can search a specific **Classification** through the **Search** option. Click the ⚙▾ button next to search to view search results based on **Classification ID, Rule Conditions, Rule Actions, Last Modified by, Modification Date, Rank** and **Actions**.

Creating a Classification Rule

You can create a classification with no condition, which will execute on all cases. You cannot create a classification without any action. After you select a condition, SOAR matches it with the alert conditions and automatically creates actions, that is defined under the **Actions** field.

Click the **Create Classification Rule** button to create a new classification. In the **Classification Editor** window, specify the details for following fields:

Matching Mode: Select <All condition, Any condition> to specify if the new rule allows all or any condition to be matched , similar to a logical AND /OR mode.

Create Conditions:

- **Type**: Select a condition type from the drop-down list. Following table presents the detailed condition types:

Type	Description
Address contains	An address value which will be searched in the IP address of alert sources. You can use the "*" character as the wildcard. Assume that this value is .*.*.22, then the condition will be met when a case is created for all the alert sources having IP addresses that end with "22".
Address doesn't contain	Condition will be met when the value typed here is not a part of alert source IP addresses.
Address is in subnet	A subnet value, which will be searched in the subnet address of alert sources. You can use the __*__ character as the wildcard.
Address is not in subnet	Condition will be met when the value typed here is not a part of alert source subnet addresses.
Address matches regex	Condition will be met when the IP address of the alert source is matched to the regular expression specified here.
Address doesn't match regex	Condition will be met when the IP address of the alert source does not match the regular expression specified here.
Alert is manual	Condition will be met when the alert is created manually.
Alert is not manual	Condition will be met when the alert is not created manually.

Type	Description
Alert parameter matches key value pair	Pair can be given as key=value. Condition will be met when the parameter (key) is equal to the value specified here for any alert parameters.
Alert parameter doesn't match key value pair	Condition will be met when the parameter (key) is not equal to the value specified here for any alert parameters.
Alert source is	Condition will be met when the alert source of the related case is the one selected here.
Alert source is not	Condition will be met when the alert source of the related case is not the one selected here.
Alert source rule name is any of	Condition will be met when the rule name of case's alert source is any of the selected values here. You can select multiple rule names in the **Parameters** combo box.
Alert source rule name is not any of	Condition will be met when the rule name of case's alert source is not any of the selected values here. You can select multiple rule names in the **Parameters** combo box.
Alert source rule name is in list	Condition will be met when the alert source rule name of the related case is in the list selected here.
Alert source rule name is not in list	Condition will be met when the alert source rule name of the related case is not in the list selected here.
Alert source rule name matches regex	Condition will be met when the alert source rule name is matched to the regular expression specified here.
Alert source rule name doesn't match regex	Condition will be met when the alert source rule name is not matched to the regular expression specified here.
Alert time is between (day of week)	Condition will be met when the creation time of an alert is between the dates and times selected here.
Alert time is not between (day of week)	Condition will be met when the creation time of an alert is not between the dates and times selected here.
Alert time is between (time of day)	Condition will be met when the creation time of an alert is between the times of each day selected here.

Type	Description
Alert time is not between (time of day)	Condition will be met when the creation time of an alert is not between the times of each day selected here.
Assignee is	Condition will be met when the assignee of the related case is the one selected here.
Assignee is not	Condition will be met when the assignee of the related case is not the one selected here.
Assignee is set	Condition will be met when the assignee of the related case is set.
Assignee is not set	Condition will be met when the assignee of the related case is not set.
Assignee is a member of group	Condition will be met when the assignee of the related case is a member of the group selected here.
Assignee is not a member of group	Condition will be met when the assignee of the related case is not a member of the group selected here.
Classification contains	Condition will be met when the classification typed here is in classification list.
Classification doesn't contain	Condition will be met when the classification typed here is not in classification list.
Scope item category is	Condition will be met when the scope item category of the related case is the one selected here.
Scope item category is not	Condition will be met when the scope item category of the related case is not the one selected here.
Scope item role is	Condition will be met when the scope item role of the related case is the one selected here.
Scope item role is not	Condition will be met when the scope item role of the related case is the one selected here.
Scope item value equals	Condition will be met when the scope item value of the related case is equal to the value expressed here.
Scope item value doesn't equal	Condition will be met when the scope item value of the related case is not equal to the value expressed here.
Scope item value is in list	Condition will be met when the scope item value of the related case is in the list selected here.

Type	Description
Scope item value is not in list	Condition will be met when the scope item value of the related case is not in the list selected here.
Severity is	Condition will be met when the severity of the related case is the one selected here.
Severity is not	Condition will be met when the severity of the related case is not the one selected here.
Status is	Condition will be met when the status of the related case is the one selected here.
Status is not:	Condition will be met when the status of the related case is not the one selected here.

- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

Create Actions:

- **Action**: Select an action from **Add case label** and **Change severity of Case**.

- **Parameters**: Appropriate value for the type. Select from the list or enter a value.

> The newly created Classification Rule is displayed on the Classification page and is in **Disabled** state by default. You must ensure enabling the rule before using it.

Editing and Deleting a Classification

You can edit an existing classification by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Classification Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing classification by clicking the **Delete** button under the **Actions** column.

> You cannot edit an existing condition or action. You have to delete the condition or action and create a new one.

Dispatching Cases

Select **RESPOND > Playbook > Dispatch**.

You can define a set of dispatch rules to automatically assign a case to a user or user role or a tier. After consolidation, once a case is created, you can decide to assign it to a group/ a team or a person and also add a severity to the case. If you did not assign the case to any user/group/team, the system automatically selects the playbook, based on rules and labels, and then executes it to resolve the issue.

The Dispatch page presents a list of dispatch rules that must be executed for the cases with specified conditions.

Dispatch rules are processed from top to bottom and only the first match is executed. You can view the rank of the rule (to see the order of dispatch actions to be applied to the cases), conditions of the dispatch rule, dispatch actions, and the user and date of last edits performed on the rule.

You can edit the rank of a dispatch rule through the **Rank** column and created items appears as the last item in the table.

If you do not want to remove the rule permanently, you can disable it using the **Disable** button in the list.

- Searching a Dispatch Rule

- Creating a Dispatch Rule

- Editing and Deleting a Dispatch Rule

Searching a Dispatch Rule

You can search a specific **Dispatch Rule**, through the **Search** option. Click the button next to search, to view search results based on **ID, Rule Conditions, Rule Actions, Last Modified by, Modification Date, Rank** and **Actions**.

Creating a Dispatch Rule

You can create a dispatch rule with no condition, which will execute on all cases. You cannot create a classification without any action. Once you select a condition, SOAR matches it with the alert conditions and automatically creates actions, that is defined under the **Actions** field.

Click **Create Dispatch Rule** button to create a new dispatch rule. In the **Dispatch Editor** window, specify the details for following fields:

Matching Mode: Select <All condition, Any condition> to specify if the new rule allows all/any the conditions to be matched , similar to a logical AND /OR mode.

Create Conditions: : To create conditions for the rule, click on the **Create** button within the **Conditions** box.

- **Type**

  Select the condition type from the **Type** drop-down list. Following table presents the detail condition types:

  Table: Condition Types

Type	Description
Address contains	An address value which will be searched in the IP address of alert sources. You can use the "*" character as the wildcard. Assume that this value is .*.*.22, then the condition will be met when a case is created for all the alert sources having IP addresses that end with "22".
Address doesn't contain	Condition will be met when the value typed here is not a part of alert source IP addresses.
Address is in subnet	A subnet value, which will be searched in the subnet address of alert sources. You can use the __*__ character as the wildcard.
Address is not in subnet	Condition will be met when the value typed here is not a part of alert source subnet addresses.
Address matches regex	Condition will be met when the IP address of the alert source is matched to the regular expression specified here.
Address doesn't match regex	Condition will be met when the IP address of the alert source does not match the regular expression specified here.
Alert is manual	Condition will be met when the alert is created manually.
Alert is not manual	Condition will be met when the alert is not created manually.
Alert parameter matches key value pair	Pair can be given as key=value. Condition will be met when the parameter (key) is equal to the value specified here for any alert parameters.
Alert parameter doesn't match key value pair	Condition will be met when the parameter (key) is not equal to the value specified here for any alert parameters.
Alert source is	Condition will be met when the alert source of the related case is the one selected here.
Alert source is not	Condition will be met when the alert source of the related case is not the one selected here.
Alert source rule name is any of	Condition will be met when the rule name of case's alert source is any of the selected values here. You can select multiple rule names in the **Parameters** combo box.
Alert source rule name is not any of	Condition will be met when the rule name of case's alert source is not any of the selected values here. You can select multiple rule names in the **Parameters** combo box.

Type	Description
Alert source rule name is in list	Condition will be met when the alert source rule name of the related case is in the list selected here.
Alert source rule name is not in list	Condition will be met when the alert source rule name of the related case is not in the list selected here.
Alert source rule name matches regex	Condition will be met when the alert source rule name is matched to the regular expression specified here.
Alert source rule name doesn't match regex	Condition will be met when the alert source rule name is not matched to the regular expression specified here.
Alert time is between (day of week)	Condition will be met when the creation time of an alert is between the dates and times selected here.
Alert time is not between (day of week)	Condition will be met when the creation time of an alert is not between the dates and times selected here.
Alert time is between (time of day)	Condition will be met when the creation time of an alert is between the times of each day selected here.
Alert time is not between (time of day)	Condition will be met when the creation time of an alert is not between the times of each day selected here.
Assignee is	Condition will be met when the assignee of the related case is the one selected here.
Assignee is not	Condition will be met when the assignee of the related case is not the one selected here.
Assignee is set	Condition will be met when the assignee of the related case is set.
Assignee is not set	Condition will be met when the assignee of the related case is not set.
Assignee is a member of group	Condition will be met when the assignee of the related case is a member of the group selected here.
Assignee is not a member of group	Condition will be met when the assignee of the related case is not a member of the group selected here.

Type	Description
Classification contains	Condition will be met when the classification typed here is in classification list.
Classification doesn't contain	Condition will be met when the classification typed here is not in classification list.
Scope item category is	Condition will be met when the scope item category of the related case is the one selected here.
Scope item category is not	Condition will be met when the scope item category of the related case is not the one selected here.
Scope item role is	Condition will be met when the scope item role of the related case is the one selected here.
Scope item role is not	Condition will be met when the scope item role of the related case is the one selected here.
Scope item value equals	Condition will be met when the scope item value of the related case is equal to the value expressed here.
Scope item value doesn't equal	Condition will be met when the scope item value of the related case is not equal to the value expressed here.
Scope item value is in list	Condition will be met when the scope item value of the related case is in the list selected here.
Scope item value is not in list	Condition will be met when the scope item value of the related case is not in the list selected here.
Severity is	Condition will be met when the severity of the related case is the one selected here.
Severity is not	Condition will be met when the severity of the related case is not the one selected here.
Status is	Condition will be met when the status of the related case is the one selected here.
Status is not:	Condition will be met when the status of the related case is not the one selected here.

- **Parameters**: Appropriate value for the selected condition type. Select from the list or enter a value.

Create Actions:

- **Action**: Defines case dispatch actions for the rule. Select the action from the **Action** combo box. Following are the available actions:

  ○ **Add a case label**: When selected, **Parameters** field toggles to a combo box listing the case labels defined in the system. You can choose a label from the list, so that when the case meeting the above conditions is created, it will be labeled as the

one selected here.

- **Assign to a user or group**: When selected, **Parameters** field toggles to a combo box listing the users/groups defined in the system. You can choose a user or group from the list, so that when the case meeting the above conditions is created, it will be assigned to the user or group selected here.

- **Change severity of case**: When selected, **Parameters** field toggles to a combo box listing the case severities defined in the system. You can choose a severity from the list, so that when the case meeting the above conditions is created, the cases initial severity will be changed to the one selected here.

  Click the **Save** button within the **Actions** box to add your rule action. You can add as many actions as you want.

  > You cannot edit a previously created conditions or actions. You have to delete and create a new condition and action.

- **Parameters**: Appropriate value for the selected action type. Select from the list or enter a value.

> The newly created Classification Rule is displayed on the Classification page and is in **Disabled** state by default. Enable the rule before using it.

Editing and Deleting a Dispatch Rule

You can edit an existing dispatch rule by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Dispatch Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save**.

You can delete an existing dispatch role by clicking the **Delete** button under the **Actions** column.

> You cannot edit an existing condition or action. You have to delete the condition or action and create a new one.

Working with Playbooks

Select **RESPOND > Playbooks > Playbooks**.

A **playbook** defines the automation and orchestration capability. After a case is dispatched, playbook performs the response procedure. The system can execute a fully automated playbook as well as a semi-automated playbook.

A completely automated playbook does not require any decision making from the agents. A semi-automatic model requires agent intervention for decision making or providing some extra information to the automation. So during a semi-automation procedure, SOAR handles the case resolution automatically till some point and then the control is passed to agents for decision making task and again after the decision is made, the control is handled by automation. If needed, SOAR automation can again assign the task to agent for some decision making or extra information requirement. So basically, SOAR performs orchestration and then finally makes a **Response**.

You can specify the execution priority of playbooks by setting the **Rank** values for each playbook, the smaller the rank, the higher is the priority.

Playbooks are processed from top to bottom and when a case matches, all of the playbooks with matching conditions are executed.

While designing any playbook, you must set conditions to ensure if multiple playbooks can run on the same case or not. As the playbooks running on the same case are not aware of each other, they must be designed independently such that one playbook does not interfere with another. If possible, it is recommended that a case matches with only one playbook.

- Searching a Playbook
- Creating an Advanced Playbook
- Creating Workflow Playbook
- Executing Workflow Playbooks
- Workflow Playbook Elements
- Types of Connectors in the Workflow Playbook
- Importing and Exporting a Workflow
- Editing Rank of a Playbook
- Editing and Deleting a Playbook

Searching a Playbook

You can search a specific **Playbook**, through the **Search** option. Click the ⚙▾ button next to search, to view search results based on the following attributes:

- ID
- Scenario Name
- Type
- Last Modified by

- Modification Date

- Rank

- Actions

- Disabled

Creating an Advanced Playbook

The **Advanced Playbook** allows you to write your own playbook scripts.

1. Click **Create Advanced Playbook** button.

2. In the **Advanced Playbook Editor** window, specify the details for following fields:

Value	Description
Name	Display name of the playbook.
Matching Mode	**All Conditions** means playbook will be executed if all the conditions are true. **Any Conditions** means playbook will be executed if any of the conditions is true.
Rollback Mode	Set if the action will be permanent or will be rolled back after a period of time.
case auto-close	From the combo box, you can select in which conditions the playbook will close the cases.
Conditions	Click **Create** to add a condition to this playbook. You can define multiple conditions.

3. In the black console area, you can write your playbook scripts in Python programming language.

4. To test your playbook, use the **Test** option:

   a. Select a defined alert source from the combo box.

   b. For **Value to Block**, enter a value to test your script.

   > The option **Value to Block** can be any parameter depending on your script, such as IP or email address.

   c. Click **Test**.

   Your test result is displayed on the same console.

Creating Workflow Playbook

Workflow Playbooks run automatically and follows the visual process definition. You can specify the a name to the playbook in **Playbook Name**.

While creating a Workflow Playbook, you can drag and drop elements from the right side of the page. You must enter appropriate and valid values depending on the element in the Properties tab. Each element must be connected to another except the last one.

When a case is created, a playbook with matching condition is executed. The match conditions of the Workflow Playbook are defined in the Start element of the playbook.

Executing Workflow Playbooks

Workflow Playbooks are run automatically when:

- **A new case is created**: cases are created by the Alert Rule Name Filter configuration.

- **A new alert is received**: Alerts are added to the cases by the Consolidation rules.

- **Rules of the case is updated**: Some alert sources update an existing alert for example, QRadar Offences and these can trigger an execution.

Workflow Playbook Elements

To create a visual process definition, you must map the executable instructions through the predefined workflow playbook elements. You can drag and drop following elements to create the workflow:

- **Automation Bit Usage**: Automation Bits are custom code created by the users to execute custom business logic. A detailed explanation for Automation Bit's can be found in Automation Bit section of this guide. While using bits, scope will be supplied from the **Start from here** element if **Scope Filter** variable is not used.
- **Actions Usage**: There are two kinds of actions:

  ○ Actions coming from the SOAR itself, and these actions act on cases to change it appropriately, for example, Status, Severity.

  ○ The action capabilities coming from integrations. There are different capabilities depending on the target device and all of them takes some input regarding their role in the workflow.

    Action elements are named as <Integration Name> - <Capability Name>. For example, Active Directory - Lock User.

  Actions usage have several standard properties including:

Properties	Descriptions
Title	Visible name of the element in the visual editor.
Continue on Error	In some cases an action on a device can return an error for example, network problems. In such cases , SOAR will stop the execution of the workflow entirely. If this option is selected, SOAR will continue execution even if the action has failed.
Rollback Mode	SOAR can undo the action after a set time if needed. In many devices there are limits to how many items can be blocked and most of these artifacts usefulness drops over time. Rollback future gives the SOAR users a way to control their actions and the health of the target device.
Scope Filter	The scope filter name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution.
	Some actions also have other fields and these are populated from data that resides on the target device. Such as tag's or group names.
Actions are synchronous	Therefore when a workflow processes an action element, it queues this action and after successful queueing of this action workflow will resume processing the next element. This means in an ideal SOAR, processing actions will not create a performance issue for the workflow execution. There however some edge cases that when SOAR is under heavy load or an unexpected error is present, actions might be queued but different elements are executed before these actions are finished.

- **Enrichment**: Enrichments are data gathering capabilities that will assist in case response procedures and decision making.

  Enrichments have several standard properties including:

Properties	Descriptions
Title	Visible name of the element in the visual editor.
Continue on Error	In some cases an enrichment on a device can return an error e.g network problems. In such cases SOAR will stop the execution of the workflow entirely. If this option is selected SOAR will continue execution even if the enrichment is failed.
Integration	On which integration this capability will be executed.

Properties	Descriptions
Scope Filter	This part's name can be changed from capability to capability but in essence filter will define which scope items from the alert will be included in the execution.
Do not use cache	When a workflow processes an action element, it queues this action. After successful queueing workflow resumes processing the next element. This means in an ideal SOAR, processing actions does not create a performance issue for the workflow execution. However some when SOAR is under heavy load or an unexpected error is present, actions might be queued but different elements are executed before these actions are finished.
Enrichments are synchronous	When executed they will start immediately and hold the workflow execution on this state until a result is returned. It is important to note that not every enrichment works as fast as you expect and in some cases rate limits might apply affecting the execution time of the overall workflow. Some enrichments execute and then wait for the process to be completed in the target device. These are also called asynchronous for their update part but for workflow execution they are treated as synchronous as well and will stop the execution until the response is returned.

- **Tasks**: Tasks are elements that does not have an automatic component. These elements are dependent on SOC analysts for completion. Task properties are dependant on the configuration of the task. So one or more of these properties might not appear in **Properties** tab..

  Tasks have several standard properties including:

Properties	Descriptions
Title	Visible name of the element in the visual editor.
Scope Filter	The name can be changed from task to task but in essence filter will define which scope items from the alert will be included in the execution. Filters can occur more than once and they are restricted to the Scope Item Type defined for them. So a **Network Address** type filter only works on **Network Address** type scope items.
Timeout Span	It is when the task is due, it will be defined by this property. Task will be timed out when it is due and execution will continue. If left empty, this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value.

- **Analyst's Decision**: This is the logic element and provides true/false options to the analyst.

  Analyst's decision have several standard properties including:

Properties	Descriptions
Title	Visible name of the element in the visual editor.
Description	Description of the decision.
Timeout span	This property is defined when the task will be due. When the task is due will be defined by this property. Task will be timed out when it is due and execution will continue. If left empty, this value will be taken from the Configuration Parameter **WorkflowTimeout** as a global value.
Send Additional Email for Approva	When this is checked, SOAR will send an additional email for out of SOAR interaction to the selected Analyst.
Analyst	Recipient of the approval Email.

- **Utilities**: There are three types of utility elements:

  ○ **Notification**:This element supports sending notifications to different users.

  Notifications can be sent from different channels and currently on-screen, SMS, email and windows type messages are supported. Notifications use free-form subject and a pre-defined template for the message.

  ○ **Decision**: Decision are standard logic element of the workflow. For a given predicate group in the property section, SOAR checks the alert scope and the workflow scope. If both of the scopes match, the automation returns a **true** value and the playbook is executed.

  The alert scope is defined at the **Start from here** element and workflow scope is the enrichment data that is specific to the workflow execution gathered till this point.

  ○ **User Decision**: User decisions are true/false type checkpoints and they are sent to a recipient for gathering inputs.

  The difference in the **Task Decision** and **User Decisions** can be explained as, the user decision sends the decision message to a variety of recipients. It can send the notification to a free-text e-mail address, to a user, or to an the case scope.

  User decision takes a template to form the message and expects the recipient to reply with an **APPROVE** or **DENY** option. You can create more than one template to send different set of data and messages to the relevant recipients. You can find the **User Decision Notification Email Template** as a built-in template in the **Customization Library**.

  You can also define scope restricted parameters that can be filled on the fly.

> Using a scope restricted parameter in the e-mail subject shows only the first item in the parameter. Rest of the items are appended in the body of the message. The decision must appear in the body of the reply message.

Types of Connectors in the Workflow Playbook

Every element in workflow has a pre-defined connector type. There can be one, two or three output connectors.

- **Single connector**: All actions and most other types of elements, fall into this category and after the element executes workflow continue to the next element.
- **Double connector**: Elements that contain a timeout falls into this category. First connector will lead to a successful completion of the element within the given time, these are named **then** and second connector will lead to timeout.
- **Triple connector**: User and Analyst Decision falls into this category. First two connectors will lead to true and false respectively in a successful execution and third connector will lead to timeout.

Importing and Exporting a Workflow

You can import a pre-designed workflow by clicking the **Import Workflow** tab. In **Workflow Import Editor** window, navigate to the template file, add a suitable name for the template and then click **Save** to import a workflow.

To export a workflow playbook, click **Export** option under the **Actions** tab.

> You can not export an advanced playbook

Editing Rank of a Playbook

You can define the order of execution for different playbooks by assigning a rank to it. Click **Edit Rank** option under the **Actions** tab and then modify the rank of the playbook in the respective **Rank** column.

Editing and Deleting a Playbook

To edit the previously created playbooks click **Edit** option under the **Actions** tab. In the **Workflow Playbook Editor** window, modify the visual process flow to suit you requirements.

To remove a playbook from the automation, click **Delete** option under the **Actions** tab.

Handling Repetitive Tasks With Scheduled Playbooks

Select **RESPOND > Playbooks > Scheduled Playbooks**.

You can use a **Scheduled Playbook** to close repetitive tasks or automate time-based mundane tasks.

- Searching a Scheduled Playbook
- Creating Scheduled Playbooks
- Editing and Deleting a Scheduled Playbook

Searching a Scheduled Playbook

You can search a **Scheduled Playbook**, through the **Search** option. Click the ⚙️▾ button next to search, to view search results based on **ID, Name, Type, Description, Last Modified by, Modification Date** and **Actions**.

Creating Scheduled Playbooks

To create a new scheduled playbook, click the **Create Scheduled Playbook** button. In the **Scheduled Playbook Editor** window, specify the details for the following fields:

Value	Description
Name	Display name of the scheduled playbook.
Trigger Frequency	For Trigger Frequency, select from Every minute, Every 5 minutes, Every 10 minutes, Every 30 minutes, Every hour, Every 2 hours, Every 3 hours, Custom chron value (to define your own frequency) options.

In the console area, you can type a script for the playbook using Python programming language.

After typing the script, you can test the playbook using the **Test** option. Select a defined alert source from the combo box, type a value into the **Value to Block** field, and then click **Test** . Your test results are displayed on the same console.

> 📋 The option **Value to block** can be any parameter depending on your script, such as IP or email address.

You can also refer to the API Documents at the top right of the **Scheduled Playbook Editor** window.

Editing and Deleting a Scheduled Playbook

You can edit an existing scheduled playbook by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Scheduled Playbook Editor** window is displayed.

Specify the values in editor window or edit the playbook script as per your requirement and click **Save** to modify.

You can delete an scheduled playbook by clicking the **Delete** button under the **Actions** column.

Creating Custom Business Logics

Select **RESPOND > Playbooks > Automation Bits**.

Automation Bits are custom code created that you create to execute custom business logic. ArcSight SOAR supports Python as programming language to write an automation bit.

- Searching an Automation Bit
- Creating an Automation Bit
- Editing and Deleting an Automation Bit

Searching an Automation Bit

You can search a specific **Automation Bit**, through the **Search** option. Click the button next to search, to view search results based on **ID, Name, Language, Last Modified by, Modification Date** and **Actions**.

Creating an Automation Bit

Click the **+Create Automation Bit** button to create a new automation bit. In the **Automation Bit Editor** window, specify the details for following fields:

Name: Name of the Automation Bit.

Description: Description of the Automation Bit.

Input Parameters: Starting parameters of the Automation Bit. These can be **Date**, **String** or **Scope Filter** and named here to be used in the Automation Bit. **Date** results in current time. **String** creates a parameter input field in workflow playbooks. **Scope Filter** creates a filter field in workflow playbooks.

Automation Bit's are **syncronous** and will hold the workflow executions until they are done.

> This capability, if used in unexpected ways, might create longer than usual workflow execution times and delays.

You can type your **Automation Bit** script at the Black Console.

Editing and Deleting an Automation Bit

You can edit an existing automation bit by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Automation Bit Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing automation bit by clicking the **Delete** button under the **Actions** column.

Managing Triggers

Select **RESPOND > Playbooks > Triggers**.

Triggers are mini playbooks that are triggered by several events. These events are created by human interaction or passage of time where SLA is concerned. Triggers evaluate the changes in the cases and if it matches to a trigger execution condition, the trigger starts automatically. Trigger executions are done from **top to bottom** and all triggers that matches the conditions will run. Only **Event Type** condition can be used in trigger **Start Condition** and the rest of the execution is done in the workflow through **Decision** elements.

As events can not be matched to two different **Event Type**, so **AND** operator is not supported.

- Searching a Trigger
- Creating a Trigger
- Importing and Exporting a Trigger
- Editing and Deleting a Trigger

Searching a Trigger

You can search a specific **Trigger**, through the **Search** option. Click the button next to search, allows you to view search results based on **ID, Name, Last Modified by, Modification Date, Rank** and **Actions**.

Creating a Trigger

To create a trigger, click the **Create Trigger** button. In the **Trigger Playbook Editor** window, drag and drop the elements to create a workflow. To understand more on creating workflow, see **Creating Workflow Playbook.**

Importing and Exporting a Trigger

You can import a pre-designed trigger by clicking the **Import Trigger** tab. In **Trigger Import Editor** window, navigate to the template file, add a suitable name for the template and then click **Save** to import a trigger.

To export a Trigger playbook, click **Export** option under the **Actions** tab.

Editing and Deleting a Trigger

You can edit an existing Trigger by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Trigger Playbook Editor** window is displayed. Modify the properties of the Trigger Playbook elements or add or delete the element as per your requirement and then click **Save**.

Handling Manual Processes Through Tasks

Select **RESPOND > Playbooks > Tasks**.

Tasks are a way to define manual processes for Case response. The system can handle the automatic and manual elements together in a defined workflow. Analyst Task creates a task that is handled by the SOC Analysts within the SOAR Case Management.

- Searching a Task
- Creating a Task
- Editing and Deleting a Task

Searching a Task

You can search a specific **Task** through the **Search** option. Click the ⚙▾ button next to search, to view search results based on **Name, Description, Task Scopes, Task Output, Last Modified by, Modification Date** and **Actions**.

Creating a Task

You can define the **Analyst Tasks** in this window and the resulting task can then be used in the workflow as a standard element. To create a task, click the **+Create Analyst Task** button. In the **Analyst Task Editor** window, specify the details for the following fields:

Name: Visible name of the element in the visual editor.

Description: Description of the Task to be shown to the analyst.

Task Scope: Task scope is enabled here and these items will be filtered and shown to the analyst and expected to be completed by him/her.

Scope Item Categories: Input scope item types are selected here. This area supports multiselection.

Task Output: Task output is enabled here.

Scope Item Category: Expected scope item type is selected here. Scope item's created by the analyst will have this type. This area is single selection.

Task Merge: If in a case has more than one alert or a consolidation is ongoing it is possible that the workflow will run more than once and there will be tasks recurring for the analyst to complete. **Task Merge** gathers tasks occurring from the same workflow and shows them as one task to the analyst reducing their load. **Timeout Span** will be merged as well and SOAR will update the merged tasks **Due Time** as the most current one.

Using Task Output or Analyst Decision will disable **Task Merge** capability of SOAR for that elements. **Task Scope** is limited to handle **200** scope items. A task containing more than 200 scope items will be divided into more than one task.

Editing and Deleting a Task

You can edit an existing task by clicking the **Edit** button under the **Actions** column. When you click the **Edit** button, **Analyst Task Editor** window is displayed. Specify the values in editor window as per your requirement and click **Save** to modify.

You can delete an existing task by clicking the **Delete** button under the **Actions** column.

Managing Out Of The Box Workflows

Select **RESPOND > Playbooks > Workflow Templates**

> You must be an Administrator or a Superuser to create or import playbooks.

Out of the Box Playbooks provide the templates to help you design and implement your playbook. These templates are pre-designed workflows and provide guidance to customize automated response as per your requirements.

List of Out Of the Box Playbooks

ArcSight SOAR provides the following out of the box playbook templates:
- Access Attempts on Unidentified Protocols and Ports
- Admin Account Check
- Block Malicious IPs - CheckpointFW
- Block Malicious IPs - Palo Alto Panorama

- Check IP Reputation from Multiple Sources
- Command and Control Traffic-1
- Command and Control Traffic-2
- Command and Control Traffic-3
- Command and Control Traffic-4
- Endpoint Investigation - Windows
- Internal Scanning Device
- Multiple Authentication Failure
- Outbound Traffic to Suspicious Countries, Ports, Services
- Phishing Email
- Stolen-Lost Device
- Virus Traffic in the Network
- Investigate Suspicious User Account on OKTA
- APIVoid URL Enrichment
- Email Address Enrichment and Block on Cisco Ironport
- Email Address Enrichment and Block on FortiMail
- Email Address Enrichment and Block on Sophos XG
- Email Address Enrichment and Block on Symantec GW
- Investigate File Hashes & Block on Carbon Black
- Investigate File Hashes & Block on Checkpoint R80
- Investigate File Hashes & Block on Kaspersky SC
- Investigate File Hashes & Block on McAfee NSP
- Investigate File Hashes & Block on SEP Manager
- IP Enrichment on Free TI Databases
- URL Enrichment and Block on Check Point R80
- URL Enrichment and Block on McAfee Web GW
- URL Enrichment and Block on Palo Alto Panorama
- URL Enrichment and Block on Sophos XG

Prerequisites for Out of the Box Playbook:

To configure and use out of the box playbooks, a set of integrations/analyst tasks/lists, as listed in respective playbook guides, must be configured on your environment. You can also view the overview and prerequisites of each Out of the Box Playbook in the **Workflow Template** tab in the SOAR application.

Customizing Out of the Box Playbooks

The out of the box playbooks must be customized to create a playbook as per your requirement.

To customize out of the box playbooks:

1. Click **Workflow Template** tab.

2. Click **Create Workflow** and specify a name to the workflow in **Create Workflow From Template**window.

3. After importing the playbook as a template, select it and click **Repair** to configure as per your requirements.

4. Set parameter values as specified in the respective Playbook guide, in the **Workflow Repair Wizard** window.

System Status

To help you understand the system state, SOAR enable you to view the list of all alerts, action and rollback queues, action history, enrichment history, process queues and troubleshooting options.

You can monitor the system state by viewing the action and rollback queues, alerts, actions, process queues, and logs on the **Status** page.

When you click the **Status** tab, following tabs are displayed:

Displaying Alerts

Select **RESPOND** > *Status* > *Alerts*.

To understand the SOAR system status, you can view all the alerts that the system has ingested within last 30 days. You can also customize the alerts display list using filter parameters.

Customizing the Alerts Display List

You can view selected alerts by selecting the appropriate filter option.

You can select an alert source in the **Alert Source** combo box and see the alerts only generated by the selected source. You can also narrow down the alert list by providing a time interval (Start/End Dates) and specific parameters (Alert Parameters) that are included in the alerts' context.

After selecting the alert filters, a list of alerts is displayed with following details:

Parameter Name	Description
ID	Alert ID
Created At	Date and time of the alert creation.
Alert Source	This is the visible name of the alert source. A visible name is assigned to an alert source during its configuration on SOAR platform.
Cases	The Cases related with the alert. When SOAR ingested this alert, this Case is created.
Selected Alert Parameters	Some of the parameters of the alerts.
Actions	Alert Details: Click the button to view alert details. In the **Alert Details** page you can view scope items associated with this alert along with the detailed information on alert source, time and date to create and update the alert.
	Show Parameter as Json: Click the button to view all the alert data in JSON format.
	Show Executed Playbooks: Click the button to view the playbook that was run for this alert.
	Process Again: Click the button to re-evaluate all the playbooks and if SOAR finds any new playbook or updated playbook with the matching condition, it will run the playbooks again for this alert.

Action and Rollback Queues

Select **RESPOND** > **Status** > **Action and Roll backQueue**.

SOAR has a mechanism to manage actions to be executed on the integration, called queuing. This section explains the action and rollback queues.

When SOAR receives an alert, alert is processed according to playbooks and SOAR decides the action and target integration.

SOAR adds this action process or rollback process to **Action and Rollback Queues** list which you can ignore approve or clear items. In order to filter list based on process type, Integration type, you can use buttons on the top of the list.

Action History

Select **RESPOND** > **Status** > **Action History**.

Action History tab lets you display and search logs of executed actions and rollback operations. To manage action history, click on the **Action History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria:

- **Stage**: Stage of the action. Available values are **Executed Actions** and **Rollback Actions**.

- **Device**: You can select a device defined on your system to see the actions only performed on that device.

- **Playbook**: You can select a playbook defined on your system to see the actions only performed as a result of that playbook.

- **Status**: Status of the action. Available values are **All**, **Successful** and **Failed**.

- **Start/End Dates**: You can refine the action list by providing start and end dates of actions using the calendar buttons at both fields.

- **Action Value (Contains)**: A value to filter the action list where the action text contains this value.

There is a **Refresh** button on top right of the **Stage** field. You can click on this button to update the filtered actions list at that moment, or choose one of the predefined intervals in the button's dropdown list to update the list automatically at the selected interval.

There is also a **Download** button on top right of the list view. You can download your filtered action list as a CSV file to your computer using this button.

Enrichment History

Select **RESPOND** > **Status** > **Enrichment History**

Enrichment History tab lets you display and search logs of executed enrichments. To manage enrichment history, click on the **Enrichment History** tab in **Status** menu.

The page allows you to filter the action list by the following criteria as well as date:

- **All Integrations**: You can filter based on different integrations.

- **Submitters**: You can filter by users or automation.

- **Status**: Status of the enrichment. Available values are **All**, **Completed**, **Failed**, **Long Running**, **Not Started**, **In Progress** and **Excluded.**

There is a **Refresh** button on top right. For each entry there's also a **Result** column that will include a **Show** button to display the raw result of the enrichment.

Process Queues

Select **RESPOND** > **Status** > **Process Queues**.

Process Queues tab contains the following queue sub-tabs:

- **Alert Queue**: Lists the alerts received from any alert source that are saved in the SOAR database (including base events for applicable alert sources) and waiting to be processed (create/update Cases, execute playbooks).

  You can use the **Clear** button at the very end of queue list to clear the items in the respective queue.

- **ArcSight Listener Queue** : Lists the messages received from ArcSight Enterprise Security Manager that are waiting to be processed and auto-enriched before they are added to the alert queue.

Data Visualization through Dashboards and Reports

The SOAR Capability enables you to track statistical details using the dashboard and case details using the report features. You can use a predefined report template or create your own template to generate a report.

Generating SOAR Reports

The Reports Portal includes out-of-the-box reports that aid you in managing current and closed cases. Note that the reports that you previously generated with Jasper report engine will be deprecated.

Out-of-the-Box Reports

The following is the list out-of-the-box reports:

> To generate reports, you must have a **Reports** permission.

- Closed Cases Report
- Integration History report
- Integration Summary Report
- Open Cases Report

Closed Cases Report

Lists the closed cases in the specified timeframe.

Integration History Report

Along with its detailed counterpart, provides a list about all integrations or a selected integration.

Integration Summary Report

Summarizes alert sources and device integrations that exists on SOAR in the specified timeframe.

Open Cases Report

Lists the open cases in the specifiedtimeframe.

Designing Report Templates

Select **RESPOND** > **Configuration** > **Report Templates**.

You can use the Reports Portal to design you own report template. You can upload it on SOAR to get the customized reports.

Creating a Report Template

Click the **Create Report Template** button to create a new report template. In **Report Template Editor** window, specify the **Report Type Name** and navigate to the file to be uploaded.

Managing Your Service Provider Contracts

To use this feature, you must have an MSSP contract with OpenText. Not available to customers in the ArcSight SaaS environment

Select **ADMIN** > **Contract & Usage**.

OpenText provides a **pay-per-use program** for Managed Security Service Providers (MSSPs). This program offers our Partners a more affordable "pay as you go" option instead of maintaining of a perpetual license that requires a large initial investment.

The system helps you submit reports about daily and monthly average EPS (events per second) usage. You simply enable the MSSP feature, create an MSSP profile, and add contracts.

To get started, select **Add Contract**. To enable the MSSP feature, see the *Quick Start to Reporting EPS Usage*.

Managing Your MSSP Contracts

Not available to customers in a SaaS environment

Select **ADMIN** > **Contract & Usage** > **Contracts**.

OpenText provides a pay-per-use program for Managed Security Service Providers (MSSPs). This program offers our Partners a more affordable "pay as you go" option instead of maintaining a perpetual license that requires a large initial investment.

Understand MSSP Contracts

Select **ADMIN** > **Contracts & Usage** > **Contracts**.

A Partner subscribes to an OpenText MSSP contract to pay-per-use, with an entitlement of one or more of the ArcSight capabilities but without the initial cost of deploying the ArcSight Platform in your IT environment. Each contract has a set length of time before it expires. You can access and use the system as long as you have a valid contract.

The MSSP contracts charge you basis EPS (events per second) usage. OpenText bases the fee on a tiered rate. The more daily average EPS you have, the less each event costs you. Monthly average EPS and cost do not impact the total cost but are an aggregate of the daily EPS and cost. If you have few events, OpenText charges you more for the service. You can see the tiers and the rates for each tier in ArcSight Platform. The Tier Rates section lists the different tiers and the cost per EPS.

Add or Update a Contract

Select **ADMIN** > **Contract & Usage**.

After you purchase an MSSP contract from OpenText, you receive a copy of that contract. You must add the contract received to ArcSight Platform you purchased. The contract also includes a signature file that OpenText uses to verify whether the contract you added is valid or not.

When you add the contract to ArcSight Platform, OpenText verifies it and does not rely on the application's verification.

1. Click **Add Contract**.

2. Drag the contract and drop it in the box.

   or

   Click **Browse**, then browse to and select the contract.

3. (Optional) Click **Update** to modify an active contract.
4. (Optional) Click **Remove** to delete a pending future contract only.

5. Follow the instructions to complete the process.

   > If your contract expires or is going to, request OpenText for a new contract file.

Reviewing and Reporting EPS Usage

Not available to customers in a SaaS environment

Select **ADMIN** > **Contract & Usage** > **Monthly Usage Details**.

You can view your events per second (EPS) usage and the rates that OpenText charges in a single location. The system provides daily averages of your usage and an aggregate of your month-over-month usage and rates.

> ⚠️ It is possible that the bill you receive from OpenText might not match the cost displayed in the monthly report that you send to OpenText. The monthly report provides usage information, but OpenText could adjust the total cost, which results in a different invoiced amount. If you have any questions, please contact your OpenText representative.

Review Monthly Usage

Select **ADMIN** > **Contract & Usage** > **Monthly Usage Details**.

The system provides daily averages of your usage, an aggregate of your month-over-month usage and rates along with monthly usage reports and a yearly rate. The reports show the daily usages where the monthly value is an average of the daily use.

The monthly usage view provides usage or cost details. You can switch between the two views by clicking Usage or Cost in the upper-right corner.

> 📓 For various views available, the system rounds off usage and cost figures to two decimal places for easier on screen and print representation, but uses actuals in all calculations for accuracy.

1. (Optional) To view data for a different year, change the value for **Showing data for the year** at the top of the chart.

   By default, the system shows data for the current year.

2. Click **Usage** or **Cost** to view the daily average EPS usage or cost.

3. Review the usage or cost:

   Average Daily EPS (Aggregate)
   The Average Daily EPS (Aggregate) chart displays an average of your daily usage or cost. It then displays an aggregate (sum) of your month-over-month usage or the cost of your usage.

   Monthly Overview Table
   The Monthly Overview table displays your customers, their usage, their daily usage in a graph, their cost, and their month-over-month usage. You can download or email a PDF or CSV version of the report.

Submit an EPS Usage Report

Select **ADMIN** > **Contract & Usage** > **Monthly Usage Details**.

The system provides EPS usage reports that you can download or email in PDF or CSV format for your use. Each report is associated with a particular month of the selected year. It also allows you to automatically perform additional actions with these reports. You can:

- Create an email distribution list for the reports.

- Automatically send the monthly usage report to OpenText and the email distribution list.

- Set up a monthly reminder for sending the reports.

> To email PDF or CSV files from the system in a non-SaaS environment, your Arcsight Platform administrator must configure an SMTP server .If the server is not configured or available, you can still add the email addresses but the system will not be able to send the emails. For more information, see "Connecting to Your SMTP Server" in the *Administrator's Guide for ArcSight Platform*.

These reports contain a signature file that accompanies the email distribution or download of the PDF or CSV file to ensure that it has not been modified. Your browser might therefore prompt you to download more than one file when you attempt to as it includes the signature. When this occurs, agree to proceed.

To submit an EPS usage report:

1. In table row of the specific month that you want to report, select ….

2. Select the format for downloading or emailing the report:

   - **Download as CSV**

   - **Download as PDF**

   - **Email PDF**

   > Individuals on the email distribution list can ignore the signature file that accompanies the sent report.

Managing Your MSSP Profile

Not available to customers in a SaaS environment

Select **ADMIN** > **Contract & Usage** > **Profile**.

The MSSP Profile shows your account number and name from the contract, along with your contact information, while the system distributes the usage reports. You cannot access any of the sections of the MSSP Profile unless you add your contract to the system. Also, to support emailing reports, your admin must set up an SMTP server as described in Connecting to Your SMTP Server in the *Administrator's Guide to ArcSight Platform 23.3*.

Edit the MSSP Profile

Select **ADMIN** > **Contract & Usage** > **Profile**.

To be able to distribute the usage reports, you must set up your MSSP profile. Before you can set up your profile, you must add a contract. Your MSSP profile contains your account number and name from the contract, your contact information, and how you want to distribute the reports. The first time you log in, you must edit the partially configured MSSP profile to have the system email the usage reports.

1. Click **Edit**.

2. Use the following information to set up or edit your profile:

   MSSP Identification
   Verify that the console displays your correct account information from the contract. You cannot edit these fields. If there is an issue, contact your sales representative.

   Contact
   Specify the name, title, phone number, and email address of the contact person if anyone has questions about the usage reports.

   Security Ops Center (SOC)
   Specify the SOC Identifier (name) and country of the SOC you are using for ArcSight Platform.

3. (Optional) Configure how you want to distribute the usage reports.

4. Click **Save** to save your configuration information.

Configure Distribution of the Usage Reports

Select **ADMIN** > **Contract & Usage** > **Profile**.

The following information helps you configure how to distribute the usage reports. The Platform administrator must set up an SMTP server for the emails to work. You can add the email addresses without the SMTP server configured but the system does not send the emails, then.

- Send Reports Automatically
- Set Up a Monthly Reminder
- Create an Email Distribution List

For more information about setting up an SMTP server in a non-SaaS environment, see Connecting to Your SMTP Server in the *Administrator's Guide to ArcSight Platform 23.3*.

Send Reports Automatically

ArcSight can automatically send the usage reports to OpenText and your email list. The system sends the reports on the first day of each month or on the day of first login, the same month.

1. Click **Edit**.

2. Under **Email Usage Reports** > **Email Settings**, enable **Automatically email usage reports**.

3. **Save** your changes.

Set Up a Monthly Reminder

If you chose not to automatically email usage reports, you can configure a reminder email to be sent to you so that you can send the email to OpenText and any other users.

1. Click **Edit**.

2. Under **Email Usage Reports** > **Email Settings**, enable **Remind me every month**.

3. **Save** your changes.

Create an Email Distribution List

ArcSight allows you to create an email distribution list to make it easy to send the usage reports to the appropriate people.

1. Click **Edit**.

2. Under **Email Usage Reports** > **Email List**, click **Add Email Address**.

3. Specify the appropriate emails addresses.

4. **Save** your changes.

Accessing ArcMC

Available only with ArcSight capabilities. Not available in the ArcSight SaaS environment.

Select **ARCMC**.

ArcSight Management Center (ArcMC) enables you to manage and monitor ArcSight infrastructure components, particularly useful when you have a large deployment ArcSight connectors. From the **ArcMC dashboards**, you can view the health and status of the components that ArcMC manages. The **Bulk Operations** feature allows you to modify the properties of, ensure the security of, gather log information about, and restart managed components.

Accessing Bulk Operations

You must have the ArcSight Management Center deployed to use Bulk Operations.

Select **ARCMC** > **Bulk Operations**.

Bulk Operations enables you to view and manage collectors, hosts and locations of hosts, and Transformation Hubs. You can modify the properties of, ensure the security of, gather log information about, and restart managed components.

Accessing ArcMC Dashboards

Select **ARCMC** > **Dashboards**.

The dashboards enable you to view the health and status of the components that ArcMC manages.

Managing Users

You can add users or groups of users; create roles; and assign permissions to the roles for users and groups. There are default roles with appropriate permissions to use the product. If you manage groups, you can view their assigned permissions, roles, and users.

If you have the *Manage Roles* permission, you can change the permissions of any role assigned to your account except for those of the *System Admin*.

Managing Users and Groups of Users

You must have the appropriate permissions *to perform these functions.*

Click **ADMIN** > **Users and Groups**.

To delegate responsibility of managing large numbers of users across multiple managers, you can create groups. You can assign one or more managers to a group of users. Then managers assign roles to users in their groups.

View Details of a Group

You can view the details of a group. As the manager of a group, you can also modify the group's settings.

1. Click **ADMIN** > **Users and Groups** > group_name.

2. (Conditional) As a manager of the group, you can also perform the following actions:

   - Add or remove users from this or other groups

   - Assign or remove roles for users in the current group

   - Add or remove managers from the current group

     > If you have the *System Admin* role, you can add and remove managers regardless whether you manage the group.

Create a New Group

1. Click **ADMIN** > **Users and Groups** > **Create Group**.

2. Specify a name for the group, then press **Enter**.

3. To manage the new group, perform the following actions:

   - Add users to this group

   - Assign roles to the users in this group

   - Add managers to this group

Create a New User

Users must have at least one role to ensure that they can log in.

1. Click **ADMIN** > **Users and Groups** > **Create User**.

2. Specify the email ID and name of the user.

3. Select the groups to which you want to add the user.

4. Select the roles that you want to grant to the user.

5. Click **Save**.

6. (Conditional) In a non-SaaS environment, specify the user's password.

> If SMTP is configured, the system notifies the new user over email to set up a password.

View a User's Profile

The user profile provides basic details about the user. If you are a manager of the user's account group, you can modify the user's account. You must also have appropriate permissions to make the modifications.

1. To find the user, perform one of the following actions:

   - Click **ADMIN** > **Users and Groups** > **Search Users**.

   - Click **ADMIN** > **Users and Groups** > group_name.

2. Select the user that you want to view.

3. (Optional) Modify the user's profile in one of the following ways:

   - Reset the password

   - Activate or deactivate the user

- Change roles or permissions
- Change group assignments

Change the User's Password

This function is not available in the ArcSight SaaS environment.

*You must have the **Change User Password** permission, and be a manager of the user's account group.*

When you reset a user's password, the user receives a notification email automatically. The email does not include the new password. You must provide the new password to the user directly.

> In a SaaS environment, administrators and managers cannot create or change a user's password. Users can specify and reset their passwords by using the Advanced Authentication service.

1. Select **Users and Groups** > **Search Users**.
2. Select the user that you just created.
3. Click **RESET PASSWORD**.
4. Enter the password.
5. Click **SAVE**.
6. Notify the user of the new password.

Change the User's Status

*You must have the **Activate/Deactivate Users** permission, and be a manager of the user's account group.*

While you cannot delete a user, you can deactivate their account to prevent them from logging in to the system.

1. Adjust the **User Status** toggle switch to indicate Active or Inactive, as needed.
2. Click **SAVE**.

Change the User's Roles

*You must have the **Assign Roles to Users** permission, and be a manager of the user's account group.*

You can only assign those roles that you currently have. However, if you have the *Manage Groups* permission, you can assign any role to these users.

1. In the user's profile, select **Roles & Permissions**.

2. Select **Assign/Remove Roles**.

3. Change the user's roles, then select **Save**.

   Each role has a defined set of permissions. To change a user's permissions, you must change the assigned role or the permissions associated with a role.

Change the User's Group Assignments

*You must have the **Assign Users to Groups** permission, and a manager of the user's account group.*

Unless you have the *Manage Groups* permission, you can only assign those groups in which you are currently a member.

1. In the user's profile, select **Groups**.

2. Select **Add/Remove**.

3. Change the user's group assignments.

Assigning Permissions to Roles

You must have the appropriate permissions to create roles and assign permissions.

Click **ADMIN** > **Roles and Permissions**.

The system provides a set of roles that you can assign to your users. You can also create new roles with any combination of the available permissions. You can assign only the permissions and roles that you have yourself.

View Available Permissions

Some permissions are available for any deployed product. Other permissions depend on the capabilities that you have deployed.

- Reports Permissions
- User Management Permissions
- ArcSight Permissions

Reports Permissions

The following table lists the permissions available when you add the Reports feature.

Function	Permissions	In the Reports Portal, allows users to…
Reports	Report Admin	View dashboards and reports Create subfolders Schedule reports Create data worksheets, dashboards, and reports View Admin reports
Reports	Design Reports	View dashboards and reports Create subfolders Schedule reports Create data worksheets, dashboards, and reports
Reports	Schedule Reports	View dashboards and reports Create subfolders Schedule reports
Reports	View Reports	View dashboards and reports Create subfolders

User Management Permissions

The following table lists the permissions needed to manage users.

Function	Permissions	Allows users to…
User Management	View Users	View the list of all active and inactive users
User Management	Create Users	View users Assign roles to users Assign users to groups
User Management	Activate /Deactivate Users	View users Change the status of a user that you manage
User Management	Change User Password	View users Change the password of a user that you manage
User Management	Change User Email	View users Change the email associated with a user

Function	Permissions	Allows users to...
User Management	Assign Roles to Users	View users Assign roles that you currently have to users that you manage
User Management	Assign Users to Groups	View users View account groups Add and remove users from account groups that you currently manage Assign users who are members of account groups that you manage to any other account group
User Management	Manage Groups	View account groups Create account groups *You are automatically added to the account groups that you create.* Delete account groups that you currently manage Add and remove managers for account groups that you currently manage Add and remove users from account groups that you currently manage Assign users who are members of account groups that you manage to any other account group
User Management	Manage Roles	View roles Create roles *You are automatically added to the account groups that you create.* Add and remove users from roles that you have Add and remove any permission assigned to you from roles that you currently have Delete roles that you currently have

ArcSight Permissions

The following table lists the permissions available when you deploy an ArcSight capability such as Log Management and Compliance.

Function	Permission	Allows users to...	Available with...
ArcMC	ArcMC System Admin *Not available in the ArcSight SaaS environment*	Perform System Admin functions	Common services
ArcMC	ArcMC Operation Admin *Not available in the ArcSight SaaS environment*	Perform all Operations functions, but does not have access to System Admin	Common services
ArcMC	ArcMC System Viewer *Not available in the ArcSight SaaS environment*	Read only access to System Admin functions	Common services
ArcMC	ArcMC Operation Viewer *Not available in the ArcSight SaaS environment*	Read only access to Operations functions	Common services
Case Management	View Own Cases	Allows a user to view the cases assigned to them	Common services
Case Management	View All Cases	Allows a user to view all cases	Common services
Case Management	Work on Cases	Allows a user modify cases and trigger manual actions	Common services
Case Management	Close Cases	Allows a user to close cases	Common services
Case Management	Create Manual Cases	Allows a user to create a new manual case	Common services
Case Management	Add Scope Items	Allows a user to add a new scope item on a case	Common services

Function	Permission	Allows users to…	Available with…
Dashboards	Share a dashboard	With the Manage Roles permission, share the current dashboard with any role Without the Manage Roles permission, share the current dashboard with any of the roles associated with the user's role	Common services
Licensing and Usage	Manage Contract	Create and edit an MSSP profile Import, update, view, and delete an MSSP contract	an MSSP license
Licensing and Usage	Access EPS Usage	Export an EPS Usage Report	an MSSP license
Operations Management	Access Database Monitoring-Overview	View high-level, summary information about the workload and health of the database	Capabilities that require the ArcSight Database
Operations Management	Access Database Monitoring-Details *In the ArcSight SaaS environment, available only to the System Operations Administrator*	View details about the health of the individual components of the distributed database system	Capabilities that require the ArcSight Database
Operations Management	Manage Storage Groups	Create and manage storage groups	Common services
Operations Management	Manage Kafka *Available only in the ArcSight SaaS environment*	Access Kafka Manager for Transformation Hub	Transformation Hub
Searches	Execute Search	Execute searches using fieldsets, custom ranges dates, and search operators	Common services
Searches	Export Search Results	Export the search results in csv format	Common services

Function	Permission	Allows users to…	Available with…
Searches	Never Expire Search Results	Configure search results to never expire	Log Management and Compliance
Searches	Never Expire Session for Real-time Searches *Available only in the ArcSight SaaS environment*	Configure the session for a real-time search to not expire while you are logged out	Real-time Threat Detection
Searches	Manage Scheduled Searches	Create and manage scheduled searches	Common services
Searches	Import / Export Search Queries	Import and export search queries	Log Management and Compliance
Searches	Import / Export Search Criteria	Import and export search criteria	Log Management and Compliance
Searches	Perform Event Integrity Check	Run an Event Integrity Check and view the results	Log Management and Compliance
Searches	Manage Outlier Models and Scoring	Create and delete Outliers models Build and pause the scoring processes	Log Management and Compliance
Searches	Manage Lookup Lists	Add, configure, view, and delete lookup lists	Common services
Searches	Manage Fieldsets	Create, edit, and delete fieldsets	Common services
Searches	Manage Search Queries/Criteria	Create, clone, edit, delete,and view all previously saved search queries and search criteria View and clone all out-of-the-box search queries	Common services
Searches	Logger Data Migration	Execute a data migration from Logger into the ArcSight Database	Common services
SOAR Configuration	Manage SOAR Playbooks	Allows a user to view and update SOAR playbooks	Common services

Function	Permission	Allows users to...	Available with...
SOAR Configuration	Manage SOAR Integrations	Allows a user to view and update SOAR integrations and related configurations	Common services
SOAR Configuration	Monitor SOAR System	Allows a user to view SOAR status pages and pending items in queues	Common services
SOAR Configuration	Configure SOAR Parameters	Allows a user to view and update SOAR configurations	Common services

Default Roles

The system provides several default roles. If you have the *Manage Roles* permission, you can change the permissions of any role assigned to your account except for those of the *System Admin*. You can also create additional roles that reflect your organization's needs.

Some permissions are available with specific functionality, such as Reports or Search, or when you have a particular license, such as for ArcSight Intelligence.

> As of the Arcsight Platform 22.1 release, some roles are no longer default roles. However, the system continues to display them if you deployed your environment before the roles were deprecated. For example, *ArcMC User*, *Guest*, *User*, and *Report User* are no longer default roles.

Default Role	Permissions
System Admin *Not available to customers in a SaaS environment*	All permissions Add, edit, and delete data sources in the Reports Portal
Admin	All **Dashboard** permissions All **Licensing and Usage** permissions All **Reports** permissions All **Searches** permissions All **User Management** permissions *Access Database Monitoring-Overview* All **SOAR Configuration** permissions

Default Role	Permissions
Analyst	All **Dashboard** permissions
	Execute Search
	Manage Fieldsets
	Manage Search Queries/Criteria
	Schedule Reports
	View Reports
	All **Case Management** permissions
System Operations Administrator	*Access Database Monitoring-Overview*
Not available to customers in a SaaS environment	*Access Database Monitoring-Details*
	All **Dashboard** permissions
	All **ArcMC** permissions
	Manage Kafka
SCIM Integration Read-Only	View Users
Not available to customers in a SaaS environment. Not created in other environments	

Create a Role with Permissions

You can group multiple permissions into a role and assign the relevant role to your users. A user must have at least one role.

You can assign only the permissions and roles that you have yourself.

1. Click **ADMIN** > **Roles and Permissions** > **Create Role**.

2. In the field in the upper left corner, specify a name for the role.

3. Press **Enter**.

4. Select the **permissions** that you want to apply to the new role.

5. To add users to the role, complete the following steps:

   a. Select the **USERS** tab.

   b. Select **Assign role to users**.

   c. Choose the users you want to add to the role.

   d. **Save** your changes.

View Details of a Role

When you view the details of a role, you can also modify the role's settings and permissions.

1. Click **ADMIN** > **Roles and Permissions** > *role_name*.

2. (Optional) Modify the role in one of the following ways:

   - Change the set of permissions

     > You can assign only the permissions and roles that you have yourself.

   - Add or remove users

   - Delete the role

Change Permissions for the Role

You can only assign permissions that you have yourself.

1. While viewing a role, select **Permissions**.

2. In the **Permissions** tab, select the permissions that you want to add or remove.

   You might need to scroll the page to see the full set of available permissions.

Add or Remove Users for the Role

You can add or remove multiple users in a role.

1. While viewing a role, select **Users**.

2. In the **Users** tab, select **Assign role to users**.

3. Select the users that you want to assign to or remove from the role.

   You can also add or remove roles for a specific user.

Delete the Role

While viewing a role, select **Remove role from users**.

You can delete any role except the *System Admin* role.

Managing Your Profile

Select **[your_ID]** > **My Profile**.

You can manage your account settings and review your assigned roles, permissions, and groups. Also, configure your preferred default settings for product behavior.

Manage Your Account

Select **[your_ID]** > **My Profile** > **Account**.

You can change your account settings. However, if your enterprise uses an external authentication method, you cannot change your password in ArcSight Platform.

Configure Your User Preferences

Select **[your_ID]** > **My Profile** > **Preferences**.

Some deployed capabilities enable you to configure preferences for commonly used settings. For example, if you regularly use the same fieldset for a Search, you can specify that set as your preferred default.

Configure Search Preferences

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.

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

Default is *Normalized Event Time*.

Search Expires in

Specifies how often you want saved searches to expire, and thus for the system to remove them from the system. You can specify a value between 1 and 365. However, your System Admin might also specify a different range. To specify a value above 365, check with your System Admin. The expiration time resets when you access the search. Resetting the expiration time includes resuming or re-running the search, as well as saving the search and changing its settings.

The default value is *7 days*. Alternatively, if you have the *Never Expire Search Results* permission, you can choose for a search to never expire. When you create or edit a search, you can override this default setting.

Session Search Expires In

Specifies how often you want session searches to expire, and thus be removed from the system. You can specify a value between 1 and 120 hours. However, your System Administrator might limit the available range. When you create or edit a search, you can override this default setting.

The expiration time for a fixed-time search resets whenever you change or run the search. For a real-time search, the expiration timer works only when you are actively viewing the search. The time resets when you interact with the real-time search, such as moving the mouse or adjusting the histogram. If you have the *Never Expire Session for Real-time Searches* permission, the system prevents your real-time search from expiring while you are logged out.

Maximum Results for a Search

Specifies the maximum number of events (the search results limit) that the search will return. You can specify a value between 1000 and 10 million. The default is *300,000*. When creating a search, you can override this preference.

Your admin can configure a system-level setting that controls the maximum number of searches (with a limit of 10 million) for all instances of ArcSight. If you enter a value outside of the system-level setting, you will receive an error message indicating that your preferred default cannot exceed the system setting.

For information about setting a global search limit in a non-SaaS environment, see "Configuring the Deployed Capabilities" in the *Administrator's Guide for the ArcSight Platform*. If you are an ArcSight SaaS customer, reach out to Support to increase the search 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.

Source Address in subnet 11.0.*

Review Your Roles and Permissions

Select **[your_ID]** > **My Profile** > **Roles & Permissions**.

You can review the roles assigned to your account, and the permissions associated with each role.

Review Your Group Assignments

Select **[your_ID]** > **My Profile** > **Groups**.

You can review the account groups to which you belong, as well as the manager of the group.

Ensuring Data Compliance

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

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

You must purchase, then import each Compliance Pack to the Reports Portal repository. For more information about the packs, see the ArcSight Solutions and Compliance Insight Package documentation site.

- Ensuring Compliance with GDPR Standards

- Ensuring Compliance with IT Governance

- Ensuring Compliance with PCI DSS

- Ensuring Compliance with NERC

- Ensuring Compliance with SOX Standards

Ensuring Compliance with GDPR Standards

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

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

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

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

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

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

Category	Dashboards	Reports
Attack Surface Analysis - Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Vulnerabilities on GDPR Systems Overview Vulnerable GDPR Assets by Vulnerability Type XSS Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems Information Leakage Vulnerabilities on GDPR Systems Password and Authentication Weaknesses on GDPR Systems SQL Injection Vulnerabilities on GDPR Systems SSL or TLS Vulnerabilities on GDPR Systems Unpatched GDPR Systems Vulnerability Summary by CVE ID Vulnerability Summary by GDPR Asset Vulnerability Summary on GDPR Systems XSS Vulnerabilities on GDPR Systems
Attack Surface Analysis - Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems
Corporate Governance	Access Activity on GDPR Systems Overview Geo Access Activity on GDPR Systems Overview Physical Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary After Work Hours Physical Access Activity on GDPR Systems Summary Physical Access Activity on GDPR Systems Summary

Category	Dashboards	Reports
Regulatory Exposure	Data Flow to GDPR Systems Data Flow from GDPR Systems Data Flow from GDPR Systems to non EU Data Flow from non EU to GDPR Systems GDPR Systems Communication with non EU Countries GDPR Systems Communication Overview High Risk Events on GDPR Systems Overview Policy Violations on GDPR Systems Overview Threat Relationship on GDPR Systems Overview Threats on GDPR Systems Overview	Data Flow from GDPR Systems Summary Data Flow from GDPR Systems to non EU Summary Data Flow from non EU to GDPR Systems Summary Data Flow to GDPR Systems Summary High Risk Events on GDPR Systems Summary Policy Violations on GDPR Systems Summary Threats on GDPR Systems Summary

Category	Dashboards	Reports
Threat Analysis - Data Store Risk	n/a	Attacks Against Databases on GDPR Systems Cassandra Vulnerabilities on GDPR Systems CRM and ERP Vulnerabilities on GDPR Systems Database Configuration Changes on GDPR Systems Database Weaknesses on GDPR Systems Elasticsearch Vulnerabilities on GDPR Systems IBM Db2 Vulnerabilities on GDPR Systems MariaDB Vulnerabilities on GDPR Systems Microsoft SQL Server Vulnerabilities on GDPR Systems MongoDB Vulnerabilities on GDPR Systems MySQL Vulnerabilities on GDPR Systems Oracle Vulnerabilities on GDPR Systems PostgreSQL Vulnerabilities on GDPR Systems Redis Vulnerabilities on GDPR Systems
Threat Analysis - Internet	Malware Found on GDPR Systems MITRE ATT&CK on GDPR Systems by GDPR Asset MITRE ATT&CK on GDPR Systems by MITRE ID MITRE ATT&CK on GDPR Systems Overview MITRE ATT&CK Relationship on GDPR Systems Overview	Firewall Blocked Events in GDPR Environment Information Leaks from GDPR Systems Malware Found on GDPR Systems

Access Activity

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

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

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

Access Activity

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

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

After Hours Access Activity on GDPR Systems Summary

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

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

- 12 a.m. to 7 a.m. Monday through Friday

- 18 p.m. (6 p.m.) to 12 a.m. Monday through Friday

- All day on Saturday and Sunday

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

Authorization Changes Summary on GDPR Systems

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

Authorization Changes Summary on GDPR Systems

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

Failed Access Activity by GDPR Assets

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

Failed Access Activity on GDPR Systems by Users

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

Failed Access Activity on GDPR Systems Summary

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

After Hours Access Activity on GDPR Systems Overview

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

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

- 12 a.m. to 7 a.m., Monday through Friday

- 18 p.m. to 12 a.m., Monday through Friday

- All day on Saturday and Sunday

Authorization Changes on GDPR Systems Overview

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

Failed Access Activity by GDPR Asset

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

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

Failed Access Activity on GDPR Systems by User

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

You must specify at least one user account in lowercase.

Failed Access Activity on GDPR Systems Overview

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

Failed Access Relationship on GDPR Systems Overview

Provides an overview of the relationship between source and destination addresses and users on events that indicate a failure login activity on GDPR systems. This dashboard

relates to GDPR Articles 5 and 25 and Recital 49.

Regulatory Exposure

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

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

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

Threat User Analysis

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

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

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

Anti-Virus Disabled on GDPR Systems Summary

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

Audit Log Cleared on GDPR Systems Summary

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

Threats Executed against GDPR Systems Summary

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

Admin Activity

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

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

Dashboards	Reports
n/a	User Creations on GDPR Environment User Deletions on GDPR Environment Users Added to a Group on GDPR Environment Users Removed from a Group on GDPR Environment

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

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

Users Added to a Group on GDPR Environment
Reports the number of user accounts added to groups over time and by whom in the GDPR environment. The table provides results by date, subject, user adding the account,

and affected group. This report relates to GDPR Articles 5, 6, 7, and 32 and Recitals 78, 82, and 84.

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

Users Removed from a Group on GDPR Environment

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

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

Attack Surface Analysis

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

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

Category	Dashboards	Reports
Attack Surface Identification	High Risk Vulnerabilities on GDPR Systems	High Risk Vulnerabilities on GDPR Systems
	Information Leakage Vulnerabilities on GDPR Systems	Information Leakage Vulnerabilities on GDPR Systems
	Password and Authentication Weaknesses on GDPR Systems	Password and Authentication Weaknesses on GDPR Systems
	SQL Injection Vulnerabilities on GDPR Systems	SQL Injection Vulnerabilities on GDPR Systems
	SSL or TLS Vulnerabilities on GDPR Systems	SSL or TLS Vulnerabilities on GDPR Systems
	Vulnerable GDPR Assets by Vulnerability Type	Unpatched GDPR Systems
	Vulnerabilities on GDPR Systems Overview	Vulnerability Summary by CVE ID
	XSS Vulnerabilities on GDPR Systems	Vulnerability Summary by GDPR Asset
		Vulnerability Summary on GDPR Systems
		XSS Vulnerabilities on GDPR Systems
Security Controls Risk Identification	DoS Attacks Against GDPR Systems	DoS Attacks Against GDPR Systems

Attack Surface Identification

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

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

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

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

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

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

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

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

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

SQL Injection Vulnerabilities on GDPR Systems Report

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

SSL and TLS Vulnerabilities on GDPR Systems Dashboard

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

SSL or TLS Vulnerabilities on GDPR Systems Report

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

Unpatched GDPR Systems

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

Vulnerable GDPR Assets by Vulnerability Type

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

Vulnerabilities on GDPR Systems Overview

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

Vulnerability Summary by CVE ID

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

You must specify a CVE ID.

Vulnerability Summary by GDPR Asset

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

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

Vulnerability Summary on GDPR Systems

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

XSS Vulnerabilities on GDPR Systems Dashboard

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

XSS Vulnerabilities on GDPR Systems Report

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

Security Controls Risk Identification

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

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

DoS Attacks Against GDPR Systems

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

DoS Attacks Against GDPR Systems

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

Corporate Governance

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **GDPR** > *Reports* or *Dashboards* > **GDPR Corporate Governance** > **Record Keeping**.

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

Dashboards	Reports
Access Activity on GDPR Systems Overview	Access Activity on GDPR Systems Summary
Geo Access Activity on GDPR Systems Overview	After Work Hours Physical Access Activity on GDPR Systems Summary
Physical Access Activity on GDPR Systems Overview	Physical Access Activity on GDPR Systems Summary

Access Activity on GDPR Systems Summary

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

After Work Hours Physical Access Activity on GDPR Systems Summary

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

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

- 12 a.m. to 7 a.m., Monday through Friday

- 18 p.m. (6 p.m.) to 12 a.m., Monday through Friday

- All day on Saturday and Sunday

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

Physical Access Activity on GDPR Systems Summary

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

Access Activity on GDPR Systems Overview

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

Geo Access Activity on GDPR Systems Overview

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

Physical Access Activity on GDPR Systems Overview

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

Regulatory Exposure

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

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

Dashboards	Reports
Data Flow from GDPR Systems	Data Flow from GDPR Systems Summary
Data Flow from GDPR Systems to non EU	Data Flow from GDPR Systems to non EU Summary
Data Flow from non EU to GDPR Systems	Data Flow from non EU to GDPR Systems Summary
Data Flow to GDPR Systems	Data Flow to GDPR Systems Summary
GDPR Systems Communication with non EU Countries	High Risk Events on GDPR Systems Summary
GDPR Systems Communication Overview	Policy Violations on GDPR Systems Summary
High Risk Events on GDPR Systems Overview	Threats on GDPR Systems Summary
Policy Violations on GDPR Systems Overview	
Threat Relationship on GDPR Systems Overview	
Threats on GDPR Systems Overview	

Data Flow from GDPR Systems

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

Data Flow from GDPR Systems Summary

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

Data Flow from GDPR Systems to non EU

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

Data Flow from GDPR Systems to non EU Summary

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

Data Flow from non EU to GDPR Systems

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

Data Flow from non EU to GDPR Systems Summary

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

Data Flow to GDPR Systems

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

Data Flow to GDPR Systems Summary

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

GDPR Systems Communication Overview

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

GDPR Systems Communication with non EU Countries

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

High Risk Events on GDPR Systems Overview

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

High Risk Events on GDPR Systems Summary

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

Policy Violations on GDPR Systems Overview

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

Policy Violations on GDPR Systems Summary

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

Threat Relationship on GDPR Systems Overview

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

Threats on GDPR Systems Overview

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

Threats on GDPR Systems Summary

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

Threat Analysis - Data Store Risk

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

GDPR requires that your enterprise establish technical and organizational standards that ensure appropriate security-to-risk levels. As part of your threat analysis, you should assess the vulnerability of data storage systems.

Dashboards	Reports
n/a	Attacks Against Databases on GDPR Systems
	Cassandra Vulnerabilities on GDPR Systems
	CRM and ERP Vulnerabilities on GDPR Systems
	Database Configuration Changes on GDPR Systems
	Database Weaknesses on GDPR Systems
	Elasticsearch Vulnerabilities on GDPR Systems
	IBM Db2 Vulnerabilities on GDPR Systems
	MariaDB Vulnerabilities on GDPR Systems
	Microsoft SQL Server Vulnerabilities on GDPR Systems
	MongoDB Vulnerabilities on GDPR Systems
	MySQL Vulnerabilities on GDPR Systems
	Oracle Vulnerabilities on GDPR Systems
	PostgreSQL Vulnerabilities on GDPR Systems
	Redis Vulnerabilities on GDPR Systems

Attacks Against Databases on GDPR System

Reports events that indicate compromise, reconnaissance, hostile, or suspicious activity against GDPR systems databases over time. The table provides results by the source GDPR IP address, IP address and host of the target system, name of the event, and

number of events. This report relates to GDPR Article 32 and Recital 49.

Cassandra Vulnerabilities on GDPR Systems

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

CRM and ERP Vulnerabilities on GDPR Systems

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

Database Configuration Changes on GDPR Systems

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

Database Weaknesses on GDPR Systems

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

Elasticsearch Vulnerabilities on GDPR Systems

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

IBM Db2 Vulnerabilities on GDPR Systems

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

MariaDB Vulnerabilities on GDPR Systems

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

Microsoft SQL Server Vulnerabilities on GDPR Systems

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

MongoDB Vulnerabilities on GDPR Systems

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

MySQL Vulnerabilities on GDPR Systems

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

Oracle Vulnerabilities on GDPR Systems

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

PostgreSQL Vulnerabilities on GDPR Systems

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

Redis Vulnerabilities on GDPR Systems

Reports vulnerabilities related to Redis on GDPR systems. The chart shows the GDPR systems with the most vulnerabilities. The table provides results by GDPR asset,

signature ID, agent severity, description of the vulnerability, and date of the most recent event. This report relates to GDPR Articles 32, 35, and 83 and Recitals 76, 77, 78, and 83.

Threat Analysis - Internet

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

GDPR requires that your enterprise establish technical and organizational standards that ensure appropriate security-to-risk levels. As part of your threat analysis, you should assess the vulnerability of firewalls, places where information might leak, and existence of malware on your GDPR systems.

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

Firewall Blocked Events in GDPR Environment

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

Information Leaks from GDPR Systems

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

Malware Found on GDPR Systems Dashboard

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

Malware Found on GDPR Systems Report

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

MITRE ATT&CK on GDPR Systems by GDPR Asset

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

MITRE ATT&CK on GDPR Systems by MITRE ID

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

MITRE ATT&CK on GDPR Systems Overview

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

MITRE ATT&CK Relationship on GDPR Systems Overview

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

Ensuring Compliance with IT Governance

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002**.

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

We provide the **Compliance Pack for IT Governance** to help you comply with Controls 6, 8, 9, 10, 12, 13, 14, 16, and 17. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

This package includes dashboards and reports organized by the ISO-27002 requirements:

Category	Dashboards	Reports
IT Governance – Executive Overview	Overall Risk Management	n/a
6 – Organization of Information Security	n/a	Suspicious Activity in Wireless Network
8 – Asset Management	n/a	Network Active Assets New Hosts New Services
9 – Access Control	User Account Management	Account Lockouts by User All Login Activity Authentication with Null Sessions Authorization Changes Privileged Account Changes Removal of Access Rights Successful Brute Force Logins Unauthorized User Access to Network Domain User Account Creation User Account Deletion
10 – Cryptography	n/a	Insecure Cryptographic Storage Invalid Certificates Systems Providing Unencrypted Services

Category	Dashboards	Reports
12 – Operations Security	Authentication Errors	Account Activity Summary
	Database Events	Administrative Actions Events
	Events and Incidents that have Occurred	Administrative Logins and Logouts
	Malware Activity	Application Configuration Modification
	Scans Overview	Audit Log Cleared
	Vulnerabilities Management	Authentication Logins with Insecure Ports
	Vulnerability Scans and Unauthorized Access	Blocked Firewall Traffic
		Changes to Operating System
		Covert Channel Activity
		Device Configuration Changes
		Device Logging Review
		Exploit of Vulnerabilities
		Failed Administrative User Logins
		Failed Antivirus Updates
		Failed File Access
		Failed File Deletions
		Failed User Logins
		Fault Logs
		File Changes in Production
		Firewall Configuration Changes
		Logins to Database Machines
		Machines Conducting Policy Breaches
		Malicious Code Sources
		Network Device Configuration Changes
		Policy Violations
		Resource Exhaustion
		Software Changes in Production
		Successful Administrative User Logins
		Successful File Deletions
		Successful User Logins

Category	Dashboards	Reports
		Suspicious Activity
		Trojan Code Activity
		User Actions All Events
		User Logins and Logouts
		Virus Infected Machines
		Vulnerabilities Scanner Results
13 – Communications Security	Email Activities Peer to Peer Activity Phishing Activities	Accessed Ports through Firewall Firewall Open Port Review Information Interception Events Insecure Services Interzone Traffic Organizational Information Leaks Personal Information Leaks Processes by Asset
14 – System Acquisition, Development, and Maintenance	n/a	Invalid Data Input
16 – Information Security Incident Management	Internal Reconnaissance	Confidential Breach Sources Denial of Service File Integrity Changes Information Systems Failures Integrity Breach Sources Internal Reconnaissance by Event Internal Reconnaissance by Source Address Internal Reconnaissance by Target Address
17 – Information Security Aspects of Business Continuity Management	n/a	Availability Attacks

IT Governance – Executive Overview

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Dashboards** > **Overview**.

To help individuals in management and C-suite positions to quickly understand the current state of your enterprise's compliance with ISO-27002 controls, you can view the following dashboard:

Dashboards	Reports
Overall Risk Management	n/a

Overall Risk Management
Provides, in charts, the overall risk score of your IT environment. You can view the most assets at highest risk, risk score by ISO control, and the rules triggered by an ISO control.

6 – Organization of Information Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002 > Reports** > **ISO 6 – Organization of Information Security**.

Control 6: *Organization of information security* of the ISO 27002 standard focuses on ensuring that your organization supports and maintains information security operations, both on- and off-site.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Suspicious Activity in Wireless Network

Suspicious Activity in Wireless Network
Reports events that indicate suspicious activity in the wireless network. For example, a malicious user might scan ports to discover open doors or weak points in the wireless network. The table provides results by the type of suspicious activity, details about the target and source systems, and the number of events.

In the logical model, use the **iDestinationWirelessNetwork** variable to specify wireless networks. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

8 – Asset Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 8 – Asset Management**.

Control 8: *Asset Management* of the ISO 27002 standard focuses on identifying the physical and information assets in your enterprise, and determining the appropriate level of protection necessary for each.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Network Active Assets New Hosts New Services

Network Active Assets
> Reports all hosts that have been included as the source address in logged events. The table provides results by the source IP address, user, and zone; the number of events; and when the event occurred.

New Hosts
> Reports all new hosts on the network detected by traffic analysis systems. The table provides results by the host name, IP address, and zone of the target system and when the event occurred.

New Services
> Reports all new services on the network detected by traffic analysis systems. The table provides results by the service name, IP address, and host name; the port used, the number of events, and when the most recent event occurred.

9 – Access Control

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards* or *Reports* > **ISO 9 – Access Control**.

Control 9: *Access Control* of the ISO 27002 standard focuses on preventing unauthorized user access to information and the facilities that process information.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
User Account Management	Account Lockouts by User
	All Login Activity
	Authentication with Null Sessions
	Authorization Changes
	Privileged Account Changes
	Removal of Access Rights
	Successful Brute Force Logins
	Unauthorized User Access to Network Domain
	User Account Creation
	User Account Deletion

Account Lockouts by User

Reports the accounts most often locked out. The table provides results about the locked out user, the target IP address and host name, the number of event, and when the most recent event occurred.

All Login Activity

Reports all successful, failed, and attended login activity by all users in the network. The table provides results by the IP address and name of the target system, the source IP address, the user involved, the outcome of the login attempt, the number of attempts, and when the most recent attempt occurred.

Authentication with Null Sessions

Reports possible null authentication sessions where the outcome is successful, failed, or an attempt. A null session attack exploits an authentication vulnerability for Windows Administrative Shares where a malicious user connects to a local or remote share without authentication. The table provides results by the target IP address and user, the source IP address and user, the outcome of the authentication attempt, the number of attempts, and when the most recent attempt occurred.

Authorization Changes

Reports authorization changes made on systems and the number of events per host. The table provides results by the target zone, IP address, and user; the source user, the type of event, the number of attempts, and when the most recent attempt occurred.

Privileged Account Changes

Reports all changes made to privileged accounts, such as password changes. The table provides results by the event, the name and IP address of the user who made the change, and when the change occurred.

Removal of Access Rights

Reports the access rights removed from user accounts. The table provides results by the access right that was removed, the IP address and host where the change was made, the user who made the change, the number of changes, and when the change occurred.

Successful Brute Force Logins

Reports the details of successful brute force logins. The table provides results by the user logging in, the IP address and host affected, the number of logins and when the event occurred.

Unauthorized User Access to Network Domain

Reports login sessions where the user is unauthorized for the specific network domain. The table provides results by the user attempted access, the target IP address and host, the source IP address for the user, the outcome of the attempt, the number of attempts, and when the event occurred.

To specify authorized users and network domains, update the variables **isDestinationAuthorizeUser** and **isNetworkDomain**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

User Account Creation

Reports all events that indicate a user account has been added to a system. The table provides results by the IP address and host where the event occurred, the user adding accounts, the number of events, and when the event occurred.

User Account Deletion

Reports all events that indicate a user account has been removed from a system. The table provides results by the IP address and host where the event occurred, the user removing accounts, the number of events, and when the event occurred.

User Account Management

Provides, in charts, details of scans, probes, and unauthorized access. You can view the number of accounts created and deleted by the user making the change, as well as the hosts that have been added or deleted.

10 – Cryptography

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** >
ISO 10 – Cryptography.

Control 10: *Cryptography* of the ISO 27002 standard focuses on using cryptographic keys to
protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Insecure Cryptographic Storage Invalid Certificates Systems Providing Unencrypted Services

Insecure Cryptographic Storage

Reports vulnerabilities associated with insecure cryptographic storage detected on your
systems. The table provides results by IP address and name of the asset, the detected
vulnerability, and when the most recent event occurred.

Invalid Certificates

Reports events that indicate an error with a server's certificate. The chart displays the
number of such occurrences per host. The table provides results by the name of the
event, the IP address and host name of the server, the user associated with event, the
number of events, and when the event occurred.

Systems Providing Unencrypted Services

Reports the systems that provide unencrypted services. The table provides results by the
port, process, service, IP address of the system, and the number of events.

12 – Operations Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards
or Reports* > **ISO 12 – Operations Security**.

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

To assess your enterprise's compliance with this requirement, use the following dashboards
and reports:

Dashboards	Reports

Authentication Errors

Database Events

Events and Incidents that have Occurred

Malware Activity

Scans Overview

Vulnerabilities Management

Vulnerability Scans and Unauthorized Access

Account Activity Summary

Administrative Actions Events

Administrative Logins and Logouts

Application Configuration Modification

Audit Log Cleared

Authentication Logins with Insecure Ports

Blocked Firewall Traffic

Changes to Operating System

Covert Channel Activity

Device Configuration Changes

Device Logging Review

Exploit of Vulnerabilities

Failed Administrative User Logins

Failed Antivirus Updates

Failed File Access

Failed File Deletions

Failed User Logins

Fault Logs

File Changes in Production

Firewall Configuration Changes

Logins to Database Machines

Machines Conducting Policy Breaches

Malicious Code Sources

Network Device Configuration Changes

Policy Violations

Resource Exhaustion

Software Changes in Production

Successful Administrative User Logins

Successful File Deletions

Successful User Logins

Suspicious Activity

Trojan Code Activity

User Actions All Events

User Logins and Logouts

Virus Infected Machines

	Vulnerabilities Scanner Results

Account Activity Summary

Reports all account activities by type. The table provides results by the event name, the user associated with the event, the target IP address and host name, and number of events per user.

Administrative Actions Events

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

Administrative Logins and Logouts

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

Application Configuration Modification

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

Audit Log Cleared

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

Authentication Logins with Insecure Ports

Reports assets with authenticated logins that used insecure ports. This report is useful for auditors to track and identify assets that are not following the security standard. The table provides results by the insecure port, the name of the source and target systems, the target user (if any), the type of event or user, the number of events, and the date of the most recent event.

Authentication Errors

Provides an overview of the authentication failure events in your enterprise. You can view a trend of failed authentication events over time, the different outcomes of the authentication events, and the failed logins by administrative and non-administrative users.

Blocked Firewall Traffic

Reports events generated by devices that have blocked traffic. The table provides results by the target port, the source and target IP address and host name, the type of event, and number of events.

Changes to Operating System

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

Covert Channel Activity

Reports events identified as covert channel activity. These events are generated by IDS devices and could indicate the use of different tools designed to establish an undetected channel to and from your enterprise. The table provides results by the type of event, the IP address and host name of the target and source systems, and when the event occurred.

Database Events

Provides, in charts and a table, an overview of the database events. You can view the trend of events over time, events by product, by the behavior of each event, and user names, IPs involved in the events. The table lists the name of the event; the target user and associated IP address; the source user and associated IP address; the outcome of the event; and the number of events.

Device Configuration Changes

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

Device Logging Review

Reports the devices with the most logging events, such as a database. The table provides results by the device host name and address, a count of events received, and when the device most recently received an event.

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

Events and Incidents that have Occurred

Provides, in charts, an overview of the different security incidents that might indicate that systems or data in your enterprise have been compromised. You can view a trend of events by severity over time, as well as events by geographic location, the techniques used, severity, source IP address, and target IP address. You can also review the relationships between target and source IP addresses.

Exploit of Vulnerabilities

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

Failed Administrative User Logins

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

Failed Antivirus Updates

Reports number of failures in updating anti-virus software over time. The table provides results by the update that failed; the IP address, name, and zone of the target system; the type of event, and when the failure occurred.

Failed File Access

Reports the details of events that indicate failed attempts to access files. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed File Deletions

Reports information about files that failed to be deleted. The table provides results by the targeted file, the IP address and name of the target system, the type of event, the number of attempts, and when the most recent attempt occurred.

Failed User Logins

Reports the number of failed logins over time. A high number of failed access attempts can indicate malicious activity. The table provides results by account name, the name

and IP address of the host where the login failed, the affected product or operating system, the number of failures detected, and when the most recent event occurred.

Fault Logs

Reports all events indicating that a system fault has occurred over time. The table provides results by the IP address and name of the host where the fault occurred, the name of the event, the number of events, and when the most recent event occurred.

File Changes in Production

Reports changes made to files in the production network. The table provides results by the target file, the IP address and name of the host of the file, the number of events, and when the most recent event occurred.

Before using this report, you must add the systems that reside in the production network to the variable **isProductionNetwork**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

Firewall Configuration Changes

Reports events by host that indicate changes to firewall configuration. The table provides results by the IP address and zone of the firewall, the firewall rule and configuration that was changed, the number of changes, and the time that the event occurred.

Logins to Database Machines

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

Machines Conducting Policy Breaches

Reports policy breaches by system, where the event matches the category technique of `/Policy/Breach`. The table provides results by the device group, affected vendor and product, the IP address and name of the host, and when the breach occurred.

Malicious Code Sources

Reports malicious code events by host system. The table provides results by the event name, the IP address and name of the affected device, the affected product, the category of the malicious code, and the outcome.

Malware Activity

Provides, in charts, an overview of the malware events that might indicate systems or data in your enterprise have been compromised. You can view a trend of malware

events over time, as well as events by geographic location, malware category and malicious event, the affected IP addresses and hosts, suspicious IP addresses and hosts names, and target IP addresses. You can also review the relationships between target and source IP addresses. You can also review the techniques used to exploit and launch further attacks.

Network Device Configuration Changes

Reports events that indicate configuration file changes on network equipment such as routers and switches. The table provides results by the change made, the device affected, the IP address where the change originated, the IP address and name of the host where the change occurred, and when the change occurred.

Policy Violations

Reports all policy breaches by source IP address. A policy breach could be IM use or the downloading of unauthorized content. The table provides results by the affected policy, the IP address and name of the source and target hosts, the number of breaches, and when the most recent breach occurred.

Resource Exhaustion

Reports events that indicate resource exhaustion on particular hosts. A malicious user can create or exploit resource exhaustion vulnerabilities by causing the programs to crash or falter, or by interfering with the programs such that the programs do not have enough resources to perform properly. If this occurs, the systems and programs become unavailable for use. The table provides results by the IP address and name of the host where the event occurred, the type of event, the number of events, and when the most recent event occurred.

Scans Overview

Provides an overview of scan results. You can view the signatures of potential vulnerabilities, the most active scanners, and the most scanned ports and assets.

Software Changes in Production

Reports events that indicate changes to daemons, access policies, and other software changes in the production environment. The table provides results by the event, the IP address and name of the target asset, and the target user.

Before using this report, you must add the systems that reside in the production network to the variable **isProductionNetwork**. For more information, see the *Solutions Guide for ArcSight Compliance Pack for IT Governance*.

Successful Administrative User Logins

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

Successful File Deletions

Reports events that indicate successful attempts to delete files by the target IP address. The table provides results by name of the deleted file, the IP address where the file was deleted, the number of files deleted, and when the deletion occurred.

Successful User Logins

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

Suspicious Activity

Reports suspicious events in your network. The table provides results by the event name, the IP address and name of the host where the event occurred, the number of events, and when the most recent event occurred.

Trojan Code Activity

Reports all the trojan activity detected by IP address in the environment. The table provides results by the type of activity, the IP address that originated the activity, the IP address and name of the target host, and when the event occurred.

User Actions All Events

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

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

User Logins and Logouts

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

Virus Infected Machines

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

Vulnerabilities Management

Provides an overview of the vulnerabilities detected per host. You can view a trend of vulnerabilities reported over time, the most reported vulnerabilities, the assets with the most vulnerabilities, and vulnerabilities by severity.

Vulnerabilities Scanner Results

Reports vulnerabilities by type as detected by vulnerability scanners. The table provides results by the vulnerability, the IP address and name of the affected host, and the quantity found.

Vulnerability Scans and Unauthorized Access

Provides an overview of the scans, probes, and unauthorized access reported in your environment. You can view results by the systems with the most unauthorized access attempts, severity of events, the most scanned ports, the vulnerabilities scanned, and the signature of the riskiest vulnerabilities.

13 – Communications Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > *Dashboards* or *Reports* > **ISO 13 – Communications Security**.

Control 13: *Communications Security* of the ISO 27002 standard focuses on using cryptographic keys to protect the confidentiality, integrity, and availability of information.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
Email Activities	Accessed Ports through Firewall
Peer to Peer Activity	Firewall Open Port Review
Phishing Activities	Information Interception Events
	Insecure Services
	Interzone Traffic
	Organizational Information Leaks
	Personal Information Leaks
	Processes by Asset

Accessed Ports through Firewall

Reports all ports accessed through a firewall by port and number of events. The table provides results by IP address of the firewall device, the type and vendor of the firewall, and the port used.

Email Activities

Provides an overview of email activities in your enterprise. You can view the accounts by quantity of emails received and sent, as well as by the size of emails received and sent.

Firewall Open Port Review

Reports the ports open in firewalls by the number of access events per port. The table provides results by IP address of the firewall device, the type of firewall, the open port, the number of events, and when the most recent event occurred.

Information Interception Events

Reports the traffic interception events that indicate spoofing and man-in-the-middle attacks. The table provides results by the type of event, the IP address of the target and source systems, the number of events, and when the most recent event occurred.

Insecure Services

Reports the events by port number and type of insecure service, such as FTP or Telnet. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Interzone Traffic

Reports the communications that pass between different zones over time. The table provides results by the IP address, name, and zone of the target host; the source zone, the protocol used; and when the most recent communication occurred.

Organizational Information Leaks

Reports events associated with information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Peer to Peer Activity

Provides an overview of peer-to-peer communication events. You can view a trend of communications over time, the total number of communications, communications by source IP address, and the relationship of communications that occur between source and target IP address.

Personal Information Leaks

Reports events that are associated with personal information leaks as reported by IDSs over time. The table provides results by the event, the source and target users, the number of events, and when the most recent event occurred.

Phishing Activities

Provides an overview of phishing activity in your enterprise. You can view a trend of phishing events over time, events received from suspicious domains, and number of events by recipient email and sender's email.

Processes by Asset

Reports the processes running on assets in your environment. The table provides results by the IP address, name, and zone of the host where the processes are running, the process, the application protocol used, the service, the product, and the number of running processes.

14 – System Acquisition, Development, and Maintenance

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 14 – System acquisition development and maintenance**.

Control 14: *System acquisition, development, and maintenance* of the ISO 27002 standard focuses on incorporating information security throughout the lifecycle of the data. Your enterprise is expected to ensure the security of data in both test/development and product environments.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	Invalid Data Input

Invalid Data Input

Reports events that indicate corrupt data input such as exceptionally long URLs or SNMP requests that exceed the allowed buffer size.

The table provides results by the type of event, the IP address and name for both the target and source of the host, and the number of events.

16 – Information Security Incident Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **ITGov** > *Reports* or *Dashboards* > **ISO 16: Information security incident management**

Control 16: *Information security incident management* of the ISO 27002 standard expects your enterprise to effectively and consistently manage information security incidents.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
Internal Reconnaissance	Confidential Breach Sources
	Denial of Service
	File Integrity Changes
	Information Systems Failures
	Integrity Breach Sources
	Internal Reconnaissance by Event
	Internal Reconnaissance by Source Address
	Internal Reconnaissance by Target Address

Confidential Breach Sources

Reports the number of confidentiality breach events by IP addresses of the source system. The table provides results by the IP address, name, and zone of the source; the number of events; and when the most recent event occurred.

Denial of Service

Reports the number of denial of service (DoS) events by IP addresses of the targeted system. The table provides results by the IP address , name, and zone of the targeted system; the type of DoS activity; and the number of events.

File Integrity Changes

Reports changes to files where the modification might compromise the integrity of the file. The table provides results by the path to the modified file, the IP address and name of the targeted host, the number of modifications, and when the most recent event occurred.

Information Systems Failures

Reports the number of changes to monitored files by target IP address and type of change. The report includes only events where agent severity is **High** or **Very-High**. The table provides results by the type of event; the IP address, name, and zone of the targeted system; and the number of events.

Integrity Breach Sources

Reports the number of attacks associated with integrity breaches, by source IP and type of breach. The table provides results by the type of breach event; the IP address, name, and zone of the source system; the number of events; and when the most recent event occurred.

Internal Reconnaissance

Provides an overview of events that indicate internal reconnaissance, which are attacks that occur within your organization's network, systems, and premises.

Internal Reconnaissance by Event

Reports the top events by the source IP address associated with the specified internal reconnaissance events. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one event by type.

Internal Reconnaissance by Source Address

Reports the number of internal reconnaissance events associated with the specified source IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

Internal Reconnaissance by Target Address

Reports the number of internal reconnaissance events associated with the specified target IP address. The table provides results by the type of event, the IP address, name, and zone of the target and source hosts; and the number of events.

You must specify at least one IP address.

17 – Information Security Aspects of Business Continuity Management

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **IT GOV** > **ISO-27002** > **Reports** > **ISO 17 – Information security aspects of business continuity management**.

Control 17: *Information security aspects of business continuity management* of the ISO 27002 standard expects that your business practices include managing the continuity of information security.

To assess your enterprise's compliance with this requirement, use the following report:

Dashboards	Reports
n/a	Availability Attacks

Availability Attacks

Reports the number of events by targeted zone that indicate attacks to limit or prevent the availability of systems, networks, devices, or services in your enterprise. The table provides results by the type of event; the IP address, name, and zone of the targeted host; the number of events; and when the most recent event occurred.

Ensuring Compliance with PCI DSS

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

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

The PCI Security Standards Council has established standards to ensure the security of payment account data. To help you comply with the PCI Data Security Standards, we provide the **Compliance Pack for PCI**. For more information about adding the pack to the Reports repository, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

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

Category	Dashboards	Reports
1 – Maintain Firewalls to Protect Cardholder Data	Overview of Communication Activity from CDE Overview of Communication Activity to CDE	Accessed Ports Through Firewall Blocked Inbound Traffic to Card Holder Data Environment Blocked Outbound Traffic from Card Holder Data Environment Cardholder Data in the DMZ External to Internal PCI Systems Firewall Configuration Changes Inbound Traffic to the Card Holder Data Environment Internal PCI Systems to External Network Routing Configuration Changes Outbound Traffic from the Card Holder Data Environment Personal Firewall Installed Private IP Addresses Disclosure Unauthorized Access to Card Holder Data Environment Unauthorized Inbound Traffic to Card Holder Data Environment Unauthorized Inbound Traffic to DMZ Unauthorized Outbound Traffic from Card Holder Data Environment VPN Configuration Changes
2 – Do Not Use Default Security Parameters	Default Vendor Accounts Overview Insecure Services – Dashboard	Default Vendor Accounts Insecure Services – Report Misconfigured Systems Multiple Functions Implemented on a Server Software Inventory Unencrypted Administrative Accesses
3 – Protect Stored Cardholder Data	n/a	Credit Cards in Clear Text

Category	Dashboards	Reports
4 – Encrypt Transmission of Cardholder Data	n/a	Cryptographic Hash Algorithm Related Vulnerabilities Cryptographic Public Key Related Vulnerability Detected Cryptographic Symmetric Key Related Vulnerabilities Cryptographic Weak Protocol Vulnerability Detected SSL or TLS Vulnerabilities TLS BREACH Vulnerabilities TLS CRIME Vulnerabilities Wireless Encryption Violations
5 – Use and Regularly Update Antivirus Software or Programs	Antivirus Activity Malware Activities Overview	Disabled Antivirus and EDR Failed Antivirus and EDR Updates Installed Antivirus and EDR Malicious Code Activities from CDE Malware Activity Malware Activity by Host Spyware and Adware Activity

Category	Dashboards	Reports
6 – Maintain Secure Systems and Applications	n/a	Broken Authentication and Session Management Buffer Overflows Configuration Modifications by Host Cross-Site Request Forgery Cross-Site Scripting Database Configuration Changes Improper Access Control Improper Error Handling Injection Flaws Insecure Cryptographic Storage Meltdown or Spectre Vulnerable Assets Operating System Changes Outbound Communication from Development to Production Outbound Communication from Production to Development Security Patch Missing SQL Injection Vulnerabilities Use of Custom Accounts in Production
7 – Restrict Access to Cardholder Data	User Access Activity to Card Holder Data Environment	All Accesses to Cardholder Data Environment All Accesses to Cardholder Data Environment by User
8 – Assign a Unique ID to Each User	Password Policy Changes Overview Windows Account Lockout	Clear Text Password Transmission Password Policy Changes Password Policy Minimum Age Changed Successful Password Changes Terminated User Activity Terminated Users Windows Account Lockouts by System Windows Account Lockouts by User

Category	Dashboards	Reports
9 – Restrict Physical Access to Cardholder Data	Failed Physical Facility Access - Dashboard Successful Physical Facility Access	Failed Physical Facility Access - Report Physical Facility Access Attempts
10 – Track and Monitor Access to Cardholder Data	Firewall Events	Account Creation Account Deletion Account Modification Administrative Actions Events Administrative Authorization Changes Anonymous User Activity in CDE Audit Logs Cleared Clock Synchronization Problems Empty Origination of Event Failed Administrative Actions Failed Administrative Logins Failed Logins File Creations Deletions Modifications IDS Events Information System Failures Successful Administrative Logins Successful Logins to CDE Successful User Logins Successful User Logins by Host User Group Creation User Group Deletion

Category	Dashboards	Reports
11 – Test Security Systems and Processes Regularly	Attacks and Suspicious Activities Overview Vulnerabilities Scanning Vulnerability Summary Overview	Drill Down Assets with Buffer Overflow Vulnerabilities Drill Down Assets with High Risk Vulnerabilities Drill Down Assets with SSL and TLS Vulnerabilities Drill Down CSRF Vulnerable Assets Drill Down SQL Injection Vulnerable Assets Drill Down XSS Vulnerable Assets Exploit of Vulnerability File Integrity Events High Risk Vulnerabilities Information Interception Events Rogue Wireless AP Detected Traffic Anomaly on Application Layer Traffic Anomaly on Network Layer Traffic Anomaly on Transport Layer Vulnerability Summary by CVE Vulnerability Summary by Host Vulnerability Summary Overview
12 – Maintain a Policy that Addresses Information Security	Policy Violations - Dashboard	All Reporting Devices Policy Violations - Report Windows Domain Policy Changes

1 – Maintain Firewalls to Protect Cardholder Data

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

PCI Requirement 1 requires that you install and maintain a firewall configuration to protect data in a cardholder data environment (CDE). **Firewalls** control computer traffic in and out of your network, as well as to and from sensitive areas within secure or sensitive internal networks. To prove compliance with PCI DSS, you must monitor the firewalls at Internet

connections and between any demilitarized zones (DMZs). You must also monitor the devices that manage traffic.

Use the following dashboards and reports to check for potential firewall vulnerabilities in your environment.

Dashboards	Reports

Overview of Communication Activity from CDE Overview of Communication Activity to CDE	Accessed Ports Through Firewall Blocked Inbound Traffic to Card Holder Data Environment Blocked Outbound Traffic from Card Holder Data Environment Cardholder Data in the DMZ External to Internal PCI Systems Firewall Configuration Changes Inbound Traffic to the Card Holder Data Environment Internal PCI Systems to External Network Routing Configuration Changes Outbound Traffic from the Card Holder Data Environment Personal Firewall Installed Private IP Addresses Disclosure Unauthorized Access to Card Holder Data Environment Unauthorized Inbound Traffic to Card Holder Data Environment

	Unauthorized Inbound Traffic to DMZ
	Unauthorized Outbound Traffic from Card Holder Data Environment
	VPN Configuration Changes

Accessed Ports Through Firewall

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

Blocked Inbound Traffic to Card Holder Data Environment

Reports the destination ports with traffic to the CDE from non-CDE systems that has been blocked the most often. The table provides results by IP addresses for the firewall, the source system, and the destination system; the destination port; the protocol used, number of events; and when the most recent event occurred.

Blocked Outbound Traffic from Card Holder Data Environment

Reports an overview of blocked traffic from the CDE to non-CDE systems over time. The table provides results by blocked outbound traffic per firewall. It lists the IP addresses for the firewall, the source system, and the destination system; the source and destination zones; affected port; and when the most recent event occurred.

Cardholder Data in the DMZ

Reports the internal systems that send the most communications to a DMZ, or less secure environment, in the specified time range. The table provides results by IP address of the source and destination systems, the affected ports, when the events occurred, and the number of events.

External to Internal PCI Systems

Reports the external systems that are communicating directly with PCI internal systems most often. The table provides results by the IP addresses and zones of the source and destination systems, the affected port, protocol used, and the number of events.

Firewall Configuration Changes

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

Inbound Traffic to the Card Holder Data Environment

Reports the systems that allowed the most traffic to the CDE from non-CDE systems by destination address and port. The table provides results by the IP addresses for the firewall, the source system, and the destination system; the affected port; the protocol used; the number of events; and when the most recent event occurred.

Internal PCI Systems to External

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

Network Routing Configuration Changes

Reports the network routing devices that have had the most configuration changes in the specified time range. The table provides results by the IP address for the device, the type of device; the event name; number of events; and when the most recent event occurred.

Outbound Traffic from the Card Holder Data Environment

Reports the systems that allowed traffic from the CDE to non-CDE systems by destination IP address. The table provides results by the IP addresses for the device, the source system, and the destination system; the affected port; the protocol used; number of events; and when the most recent event occurred.

Overview of Communication Activity from CDE

Provides, in charts and a table, an overview of communication going out from the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Overview of Communication Activity to CDE

Provides, in charts and a table, an overview of communication coming into the CDE. You can view the target and source IP addresses, target ports, and the block source IP addresses.

Personal Firewall Installed

Reports the servers with a personal firewall installed. PCI standards require that users install personal firewall software on any device, such as a laptop, that is used to access the cardholder data environment and also might connect to the Internet when outside the PCI network. The table lists the IP address and name of the system hosting the personal firewall, as well as the more recent time that the firewall was detected.

Private IP Addresses Disclosure

Reports the RFC1918 IP addresses with the most communication with public IP addresses. The table provides results by IP address of the source and associated destination systems, the destination port, the protocol used, and the number of events.

Unauthorized Access to Card Holder Data Environment

Reports the accounts with the most unauthorized attempts to access the CDE. The table provides results by the user account, source and destination IP addresses, time the events occurred, and the number of events.

Unauthorized Inbound Traffic to Card Holder Data Environment

Reports the IP addresses in the cardholder environment that have experienced the most unauthorized traffic to the CDE from non-CDE systems. The table provides results by the source and destination IP addresses, the ports of the destination system, the protocol used, the number of events, and when the most recent event occurred.

Unauthorized Inbound Traffic to DMZ

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

Unauthorized Outbound Traffic from Card Holder Data Environment

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

VPN Configuration Changes

Reports the VPN gateways with the most changes to their configuration. The table provides results by IP address of the VPN, the policies or configurations changed, the type of VPN, and number of events.

2 – Do Not Use Default Security Parameters

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

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

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

Dashboards	Reports
Default Vendor Accounts Overview Insecure Services – Dashboard	Default Vendor Accounts Insecure Services – Report Misconfigured Systems Multiple Functions Implemented on a Server Software Inventory Unencrypted Administrative Accesses

Default Vendor Accounts

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

Default Vendor Accounts Overview

Provides, in several charts, an overview of default vendor accounts. You can view the accounts associated with the most events, account activity over time, the IP addresses associated with the accounts, and the most active vendors.

Insecure Services – Dashboard

Provides, in charts and table, insecure events by port number and IP address, activities by day, and the products that report insecure services in other systems.

Insecure Services – Report

Reports insecure events by port number. The table provides results by the target port, target process, target and source IP addresses, the target host name, the product that reported the insecure service, and the number of events.

Misconfigured Systems

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

Multiple Functions Implemented on a Server

Reports the servers that have multiple functions installed on them. For example, a server might have functions such as DNS, a Web server, and a database.

Software Inventory

Reports the software found by IP address and host name.

Unencrypted Administrative Accesses

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

3 – Protect Stored Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > **Reports** > **Requirement 3:
Protect Stored Cardholder Data**.

PCI Requirement 3 ensures that cardholder data cannot be read or used by individuals who maliciously or unintentionally access encrypted data. You must have security measures to encrypt, truncate, mask, or hash critical components of the data.

To assess your enterprise's compliance with this requirement, use the following report:

Credit Cards in Clear Text

Reports the hosts where credit card data has been detected in clear text format. The table provides results by the affected host and reporting device IP addresses, the signature ID, and when the clear text was detected.

4 – Encrypt Transmission of Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **Reports** > **Requirement 4:
Encryption Transmission**.

PCI Requirement 4 focuses on managing and maintaining the security of the card holder data when it is transmitted over open or public networks. Transmitted data should be encrypted. Malicious users can exploit vulnerabilities in cryptographic hashes and keys, as well as through SSL and TLS. For example, the Heartbleed Bug is a known SSL vulnerability.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Cryptographic Hash Algorithm Related Vulnerabilities
	Cryptographic Public Key Related Vulnerability Detected
	Cryptographic Symmetric Key Related Vulnerabilities
	Cryptographic Weak Protocol Vulnerability Detected
	SSL or TLS Vulnerabilities
	TLS BREACH Vulnerabilities
	TLS CRIME Vulnerabilities
	Wireless Encryption Violations

Cryptographic Hash Algorithm Related Vulnerabilities

Reports events by host name that indicate potential vulnerabilities related to hash algorithms. All cryptographic hashes that directly use the full output of a Merkle–Damgård

construction are vulnerable to length extension attacks. The table provides results by name of the event, host and IP address, and number of events.

Cryptographic Public Key Related Vulnerability Detected

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

Cryptographic Symmetric Key Related Vulnerabilities

Reports vulnerabilities related to cryptographic symmetric keys by the address or host name of the target asset. The table provides results by the target asset, the device vendor and product, the number of events, and when the most recent event occurred.

Cryptographic Weak Protocol Vulnerability Detected

Reports all vulnerabilities associated with weak cryptographic protocol. The table provides results by the vulnerability name, the affected assets, the number of events, and when the most recent event occurred.

SSL or TLS Vulnerabilities

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

TLS BREACH Vulnerabilities

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

TLS CRIME Vulnerabilities

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

Wireless Encryption Violations

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

number of events.

5 – Use and Regularly Update Antivirus Software or Programs

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 5: Antivirus**.

PCI Requirement 5 focuses on preventing malware, such as worms, viruses, and trojans, from infecting the cardholder data environment (CDE). This type of malware can enter the network through common business activities and processes: employee email, Internet usage, cell phones, or storage devices. Malware can then damage systems by exploiting system security vulnerabilities or trying to steal confidential information. Your enterprise should install and maintain antivirus software on all devices frequently affected by malware to protect networks from existing and emerging threats.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Antivirus Activity	Disabled Antivirus and EDR
Malware Activities Overview	Failed Antivirus and EDR Updates
	Installed Antivirus and EDR
	Malicious Code Activities from CDE
	Malware Activity
	Malware Activity by Host
	Spyware and Adware Activity

Antivirus Activity

Provides charts for an overview of antivirus activities in the CDE. You can view the trends of antivirus cleaning/quarantining attempts and failures over time, a trend of failed cleaning and the number of times antivirus has failed to update and the associated agent, and the number of events by device vendor.

Disabled Antivirus and EDR

Reports events associated with disabling antivirus and EDR programs by target host. The table provides results by the target host, the antivirus or EDR program affected, the user that disabled the program, the number of events, and when the event occurred.

Failed Antivirus and EDR Updates

Reports events where antivirus and EDR programs failed to update by target host. The table provides results by the target host, the antivirus or EDR program affected, the name and userID that disabled the program, the number of events, and when the event occurred.

Installed Antivirus and EDR

Reports events where antivirus and EDR programs are installed by type of program. The table provides results by the type of antivirus or EDR product, the location of the program, and the number of events.

Malicious Code Activities from CDE

Reports malicious code activity sent from the CDE. The table provides results by the source and target addresses, the type of event, the product, and the number of events.

Malware Activities Overview

Provides an overview of all malware activity in the CDE. You can view the trends of malware activities over time, top signature IDs, top affected systems, and the top reporting products.

Malware Activity

Reports the malware detected in the CDE. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Malware Activity by Host

Reports the malware activity by target host. The table provides results by the type of malware, the target asset, the number of events, and the when the event occurred.

Spyware and Adware Activity

Reports target hosts where spyware or adware has been detected. The table provides results by the affected asset, the type of spyware or adware, the event class, the number of events, and when the event occurred.

6 – Maintain Secure Systems and Applications

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 6: Secure Systems and Applications**.

PCI Requirement 6 sets the expectation that you apply security patches to all applications and systems in the cardholder data environment (CDE) to protect them from malicious and unintentional misuse. The patches should be evaluated to ensure that they do not conflict with current security configurations. You must also ensure that in-house development teams practice secure coding techniques. Applications that store sensitive data must be able to protect the data.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Broken Authentication and Session Management
	Buffer Overflows
	Configuration Modifications by Host
	Cross-Site Request Forgery
	Cross-Site Scripting
	Database Configuration Changes
	Improper Access Control
	Improper Error Handling
	Injection Flaws
	Insecure Cryptographic Storage
	Meltdown or Spectre Vulnerable Assets
	Operating System Changes
	Outbound Communication from Development to Production
	Outbound Communication from Production to Development
	Security Patch Missing
	SQL Injection Vulnerabilities
	Use of Custom Accounts in Production

Broken Authentication and Session Management

Reports events associated with broken authentication and session management over time. The table provides results by the target asset, name and signature ID of the vulnerability, and the number of events.

Buffer Overflows

Reports vulnerabilities associated with buffer overflows by CDE asset. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program. The table provides results by the affected asset, the detected vulnerability, the signature ID of the vulnerability, and when the most recent event occurred.

Configuration Modifications by Host

Reports modifications made to CDE assets. The table provides results by the affected asset, the type of modification, the user who made the change, the number of events, and when the most recent event occurred.

Cross-Site Request Forgery

Reports assets that might be vulnerable to a cross-site request forgery (XSRF or CSRF) attack. In an CSRF 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. The table provides results by the targeted asset and when the most recent event occurred.

Cross-Site Scripting

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

Database Configuration Changes

Reports changes to the database configuration by affected asset. The table provides results by the database host, the modification made, the user who made the change, the number of changes, and when the most recent change occurred.

Improper Access Control

Reports vulnerabilities associated with improper access controls. The table provides results by the signature ID of the event, the target asset, the number of events, and when the most recent event occurred.

Improper Error Handling

Reports vulnerabilities associated with improper handling of errors by affected assets. The table provides results by the signature ID of the event, the target asset, and when the most recent event occurred.

Injection Flaws

Reports the assets with the most injection flaws. The table provides results by the affected asset, the injection flaw and its signature ID, and when the event occurred.

Insecure Cryptographic Storage

Reports the IP addresses of systems where sensitive data is not stored securely. The table provides results by the affected asset, the event, the number of events, and when the most recent event occurred.

Meltdown or Spectre Vulnerable Assets

Reports the assets with the most Meltdown or Spectre vulnerabilities. The table provides results by the affected asset, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Operating System Changes

Reports changes to operating systems. The table provides results by the target asset, the change, the outcome of the change, and the number of changes.

Outbound Communication from Development to Production

Reports all communication sent from the development environment to the production environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the `isSourceZonePCIDevelopment` and `isDestinationZonePCIProduction` variables to indicate the respective zones for development and production.

Outbound Communication from Production to Development

Reports all communication sent from the production environment to the development environment. The table provides results by the source and target addresses, the port used, the transportation protocol, and the number of events.

In the logical model, you must edit the `isSourceZonePCIProduction` and `isDestinationZonePCIDevelopment` variables to indicate the respective zones for production and development.

Security Patch Missing

Reports assets by IP address with missing security patches. One of the most common ways to reduce your environment's attack surface is to ensure that all systems have the most recent security patches applied. The table provides results by the affected asset, the vulnerability and signature ID associated with the missing patch, the number of events, and when the most recent event occurred.

SQL Injection Vulnerabilities

Reports SQL injection vulnerabilities by asset. 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. The table provides results by the target assets, the vulnerability and its signature ID, the number of events, and when the most recent event occurred.

Use of Custom Accounts in Production

Reports events in the production environment associated with the specified list of accounts. The table provides results by the specified accounts, the target asset, the number of events, and when the most recent event occurred.

You must enter the accounts that you want to include in the report. Use commas to separate the values.

7 – Restrict Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 7: Restrict Access By Business Need to Know**.

PCI Requirement 7 focuses on controlling access to cardholder data, thus limiting access privileges only to users who need to know the data according to your enterprise's needs.

Usually, enterprises apply the principle of least privilege when granting access rights in the cardholder data environment (CDE).

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
User Access Activity to Card Holder Data Environment	All Accesses to Cardholder Data Environment All Accesses to Cardholder Data Environment by User

All Accesses to Cardholder Data Environment

Reports the most accessed hosts in the CDE. The table provides results by the target host name and IP address, the target user, the source user and address, and the number of events.

All Accesses to Cardholder Data Environment by User

Reports all access activity in the CDE by the user. By default, the report lists user activities. The table provides results by the target host name and address, the target user, the port used, the source address, and the number of events.

In the logical model, use the **isDestinationUserPCI** variable to specify the users in the CDE that you want to include in the reports. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

User Access Activity to Card Holder Data Environment

Provides, in charts and a table, an overview of user access activities in the CDE. You can view a trend of activity over time, as well as events by target users, target IP address, and source IP address.

8 – Assign a Unique ID to Each User

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 8: Unique User ID**.

PCI Requirement 8 covers identification and authentication for all access to system components in the cardholder data environment (CDE). Basically, your enterprise must maintain and monitor changes to user accounts and password policies to prevent malicious users from gaining access to the CDE through weak passwords or by changing password policies. This requirements applies to all accounts with administrative features, including

point-of-sale accounts; accounts used by vendors and third parties; and any account used to view cardholder data or access cardholder data or to access systems with cardholder data. This requirement does not apply to end-user accounts used by consumers.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Password Policy Changes Overview Windows Account Lockout	Clear Text Password Transmission Password Policy Changes Password Policy Minimum Age Changed Successful Password Changes Terminated User Activity Terminated Users Windows Account Lockouts by System Windows Account Lockouts by User

Clear Text Password Transmission

Reports events by IP address where passwords were transmitted in clear text. The table provides results by the target host name and IP address, the port used, the number of events, and when the clear text password was detected.

Password Policy Changes Overview

Provides, in charts and a table, an overview of policy changes on CDE assets. You can view a trend of changes made over time, changes to target user accounts, changes to target IP addresses, and changes by type.

Password Policy Changes

Reports changes to the password policy over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Password Policy Minimum Age Changed

Reports changes to the policy for the minimum password age over time in the CDE. The table provides results by the target IP address, the user who made the change, the change made, the number of events, and when the change occurred.

Successful Password Changes

Reports successful password changes over time in the CDE. The table provides results by the target IP address and host name, the affected user account, the number of events, and when the most recent event occurred.

Terminated User Activity

Reports user accounts that have been terminated but show successful authentication events after termination. The table provides results by the terminated account and when successful authentication occurred.

Terminated Users

Reports all user accounts terminated in the CDE by termination date. The table provides results by the terminated account and when the account was terminated.

Windows Account Lockout

Provides, in charts and a table, an overview of Windows accounts that have been locked out. You can view a trend of events over time, events by target IP address, and events by the accounts locked out.

Windows Account Lockouts by System

Reports, by host system, all Windows accounts that have been locked out. The table provides results by the target host name, IP address, domain, and user; the number of lockouts; and when the most recent event occurred.

Windows Account Lockouts by User

Reports, by user and domain, all Windows accounts that have been locked out. The table provides results by the target domain and user, the number of lockouts, and when the most recent event occurred.

9 – Restrict Physical Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 9: Physical Access**.

PCI Requirement 9 expects your organization to restrict access to devices that allow an individual physical access to the systems that store cardholder data, thus limiting the ability for malicious users to access or destroy the devices, data, systems, or hard copies.

> By default, these reports and dashboards assume all assets are associated with physical access. To specify specific locations and buildings, update the **isPCIBuilding** variable in the data worksheet for each PCI Requirement 9 report or dashboard. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Failed Physical Facility Access - Dashboard	Failed Physical Facility Access - Report
Successful Physical Facility Access	Physical Facility Access Attempts

Failed Physical Facility Access - Dashboard

Provides, in charts and table, an overview of failed attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

Failed Physical Facility Access - Report

Reports the number of failed attempt to access physical facilities by location. The table provides results by the target location, the user involved, the number of attempts, and when the attempt occurred.

Physical Facility Access Attempts

Reports the number of attempts to access physical facilities by location and user. The table provides results by the target location, the user involved, the outcome of the attempt, the number of attempts, and when the most recent event occurred.

Successful Physical Facility Access

Provides, in charts and table, an overview of successful attempts to access physical facilities. You can view a trend of access activity over time, as well as activity by reporting device, location, and user.

10 – Track and Monitor Access to Cardholder Data

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 10: Track and Monitor Data Access**.

PCI Requirement 10 focuses on tracking changes to user accounts and groups to detect and prevent data breaches within the cardholder data environment (CDE). Malicious users might create groups or accounts to grant them access to sensitive data, then delete their changes to hide their activity.

To assess your enterprise's compliance with this requirement, use the following dashboard and reports:

Dashboards	Reports
Firewall Events	Account Creation
	Account Deletion
	Account Modification
	Administrative Actions Events
	Administrative Authorization Changes
	Anonymous User Activity in CDE
	Audit Logs Cleared
	Clock Synchronization Problems
	Empty Origination of Event
	Failed Administrative Actions
	Failed Administrative Logins
	Failed Logins
	File Creations Deletions Modifications
	IDS Events
	Information System Failures
	Successful Administrative Logins
	Successful Logins to CDE
	Successful User Logins
	Successful User Logins by Host
	User Group Creation
	User Group Deletion

Account Creation

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

Account Deletion

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

Account Modification

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

Administrative Actions Events

Reports all actions, except logins, made by administrative users. The table provides results by the user name, device event class, number of events, and when the change occurred.

Administrative Authorization Changes

Reports all changes authorized by administrative users. The table provides results by the source and target user, the number of changes, and when the change occurred.

Anonymous User Activity in CDE

Reports all logins to the CDE by anonymous users. The table provides details about the user, the affected host, the number of attempted logins, and when the most recent event occurred.

By default, the report includes all users who log in to the CDE because the variable `isUserNameAnonymous` is set to *yes*. To make the report more specific, in the logical model, enter the list of anonymous users for the variable `isUserNameAnonymous`, as shown in the example. For more information, see the *Solutions Guide for ArcSight Compliance Pack for PCI*.

Audit Logs Cleared

Reports the audit logs cleared by user. The table provides results by the user, the affected host, the number of events, and when the most recent event occurred.

Clock Synchronization Problems

Reports the number of assets with clock synchronization issues over time. In SSL, clocks are used for certificate validation. A malicious user could modify the server or client clock

to disregard dates in certificates. Then that user will be able to impersonate the server forever even if the certificate expires. The table provides details about the affected asset and when the most recent event occurred.

Empty Origination of Event

Reports events in which the source, such as user, address, device or hostname, cannot be identified. The table provides results by the anomaly's name, the number of events, and when the most recent event occurred.

Failed Administrative Actions

Reports failed actions, except logins, by administrative users. The table provides results by the target user and host, device event class, the affected product, the number of failed attempts, and when the most recent event occurred.

Failed Administrative Logins

Reports the number of failed logins by administrative users. The table provides results by the target host, administrative user, and the number of failed attempts.

Failed Logins

Reports the number of failed logins by user. The table provides results by the target host, administrative user, and the number of failed attempts.

File Creations Deletions Modifications

Reports the file creations, deletions, and modifications by host. The table provides results by the asset, the type of activity, outcome of the activity, the number of events, and when the most recent event occurred.

Firewall Events

Provides, in charts and a table, an overview of firewall events. You can view a trend of firewall events overtime, the number of times a firewall rule has been hit, the firewalls by vendor, and products reporting the events.

IDS Events

Reports all events recorded by the IDSs in your enterprise. The table provides results by the IDS device, the type of event, the number of events, and when the most recent event occurred.

Information System Failures

Reports all failures associated with information systems. The table provides results by the target asset, the type of failure, the device vendor, and the number of failure events.

Successful Administrative Logins

Reports all successful logins by administrative users. The table provides results by the target asset, the user, and the number of logins.

Successful Logins to CDE

Reports all successful logins within the CDE. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins

Reports all successful logins by user. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

Successful User Logins by Host

Reports all successful user logins by host. The table provides results by the target asset, the user, the number of logins, and when the most recent login occurred.

User Group Creation

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

User Group Deletion

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

11 – Test Security Systems and Processes Regularly

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 11: Test Systems and Processes**.

PCI Requirement 11 focuses on frequently testing your processes and the security system components of your cardholder data environment, such as performing regular vulnerability

scans. PCI expects your enterprise to keep your processes and systems current with evolving security issues.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Attacks and Suspicious Activities Overview	Drill Down Assets with Buffer Overflow Vulnerabilities
Vulnerabilities Scanning	Drill Down Assets with High Risk Vulnerabilities
Vulnerability Type Overview	Drill Down Assets with SSL and TLS Vulnerabilities
	Drill Down CSRF Vulnerable Assets
	Drill Down SQL Injection Vulnerable Assets
	Drill Down XSS Vulnerable Assets
	Exploit of Vulnerability
	File Integrity Events
	High Risk Vulnerabilities
	Information Interception Events
	Rogue Wireless AP Detected
	Traffic Anomaly on Application Layer
	Traffic Anomaly on Network Layer
	Traffic Anomaly on Transport Layer
	Vulnerability Summary by CVE
	Vulnerability Summary by Host
	Vulnerability Summary Overview

Attacks and Suspicious Activities Overview

Provides, in charts and a table, an overview of attacks and suspicious events. You can view the IP addresses generating the most attacks, the systems that are the target of most attacks, a trend of attacks over time, and the top events.

Drill Down Assets with Buffer Overflow Vulnerabilities

Lists assets that might be vulnerable to buffer overflow. This type of vulnerability occurs when a developer fails to appropriately manage memory for user-controlled data. A malicious user could put more data into a pre-allocated memory buffer than the buffer can hold, dramatically impacting the operation of a program.

Drill Down Assets with High Risk Vulnerabilities

Reports assets that might be vulnerable to listed high-risk security threats. 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.

Drill Down Assets with SSL and TLS Vulnerabilities

Reports assets that might have the listed TLS or SSL vulnerability. For example, malicious users can exploit a known vulnerability in SSL with the Heartbleed Bug.

Drill Down CSRF Vulnerable Assets

Reports assets that might be vulnerable to the listed cross-site request forgery (XSRF or CSRF) attack. In a CSRF 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.

Drill Down SQL Injection Vulnerable Assets

Reports assets that might be vulnerable to the listed SQL injection attacks. 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.

Drill Down XSS Vulnerable Assets

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

Exploit of Vulnerability

Reports events that indicate an attempt to exploit a given detected vulnerability. The table provides results by the vulnerability, IP address and name of the affected system, number of events associated with the vulnerability, and when the most recent event occurred.

File Integrity Events

Reports events that indicate file integrity might be compromised in your environment. File integrity monitoring, also known as change monitoring, checks operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack. The table provides results by the signature ID, IP address and name of the affected system, the number of events, and when the most recent event occurred.

High Risk Vulnerabilities

Reports the systems with the greatest likelihood of being exploited based on the reported vulnerabilities. The table provides results by the vulnerability, the signature ID, name of the affected system, and when the most recent event occurred.

Information Interception Events

Reports traffic interception events that indicate spoofing or man-in-the-middle attacks. The table provides results by the signature ID, details of the source and destination addresses, the number of events, and when the most recent event occurred.

Rogue Wireless AP Detected

Reports rogue wireless access points (AP) found in your environment. A user might install a rogue AP unintentionally or maliciously in an office or data center without the knowledge or permission from the system administrator via the wired infrastructure. The chart shows rogue APs found over time. The table provides results by the device ID and name, when the event occurred, and the number of events.

Traffic Anomaly on Application Layer

Reports all the traffic anomalies found in the application layer. Malicious users attack the application layer of an application, which specifies the communication protocols and interface methods used by hosts in the network, to disrupt processes and services on a web server or application. The table provides results by signature ID, details of the

affected system or product, the number of events, and when the most recent event occurred.

Traffic Anomaly on Network Layer

Reports all the traffic anomalies found in the network layer. This layer supports communications by sending packets of data back and forth between different networks, and thus can be vulnerable to a large variety of attacks. The table provides results by the destination and source systems, the number of events, and when the most recent event occurred.

Traffic Anomaly on Transport Layer

Reports all the traffic anomalies found in the transport layer. In this layer, a malicious user might hijack session by taking control of a session between two nodes after the initial authentication process is complete. The table provides results by signature ID, the destination and source systems, the number of events, and when the most recent event occurred.

Vulnerability Summary by CVE

Reports vulnerabilities by CVE and severity. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary by Host

Reports vulnerabilities found by host. The table provides results by the CVE, its severity, the affected asset, and when the most recent event occurred.

Vulnerability Summary Overview

Reports all the vulnerabilities found in the PCI environment. The table provides results by the vulnerability name, CVE, the common vulnerability score (CVSS), signature ID, the affected asset, and when the most recent event occurred.

Vulnerabilities Scanning

Provides, in several charts, the details of reported vulnerabilities over time. You can view the assets with the most high-risk vulnerabilities, the most reported vulnerabilities, and the assets with vulnerabilities including the hostnames.

Vulnerability Type Overview

Provides charts for an overview of vulnerabilities by category: SQL, XSS, CSRF, SSL, high-risk, and buffer overflow. You can drill down in the charts to identify the affected assets.

12 – Maintain a Policy that Addresses Information Security

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **PCI** > *Reports* or *Dashboards* > **Requirement 12: Maintain Information Security Policy**.

PCI Requirement 12 expects your enterprise to maintain a policy that addresses the information security for all personnel who are associated with your enterprise or have some form of access to the cardholder's data system. Personnel should know the enterprise's expectations for handling cardholder data, and should know their responsibilities for protecting the sensitivity of the data.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Policy Violations - Dashboard	All Reporting Devices
	Policy Violations - Report
	Windows Domain Policy Changes

All Reporting Devices

Lists all reporting devices in the environment by number of events. PCI expects that you maintain an inventory of devices and check for unapproved devices. The table lists device by product, vendor, IP address, and zone.

Policy Violations - Dashboard

Provides, in charts and a table, an overview of policy violations. You can view the number of violations by day, the IP addresses and signature IDs associated with violations, and the users with the most violations.

Policy Violations - Report

Reports policy violations by IP address. The table lists the details of the affected host system, the number of events, and when the events occurred.

Windows Domain Policy Changes

Reports changes to the Windows domain policy by associated IP address. The table lists the details of the affected host system and the number of changes.

Ensuring Compliance with SOX Standards

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

Select **Reports** > **Portal > Repository** > **Data Compliance Content** > **SOX**.

The Sarbanes-Oxley Act (SOX) is a United States federal law that was enacted in 2002. The stated purpose of the law is to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes.

To help you comply or prove compliance with SOX, we provide the **Compliance Insight Package for SOX**. For more information about adding the package to the Reports repository, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*. The guide includes information about identifying assets that must comply with SOX.

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

Category	Dashboards	Reports
Executive Summary	Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a
ISO 5 Information Security Policies	Policy Violations Overview	Policy Violations
ISO 6 Organization of Information Security	VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity

Category	Dashboards	Reports
ISO 7 Human Resource Security	Activity by User	n/a
ISO 8 Asset Management	Removable Media Activity	n/a
ISO 9 Access Control	n/a	Account Creations Account Deletions Account Lockouts by System Account Lockouts by User Insecure Ports Insecure Services Password Policy Changes Password Weaknesses User Group Account Creations User Group Account Deletions
ISO 10 Cryptography	n/a	SSH Vulnerabilities SSL or TLS Vulnerabilities VPN Vulnerabilities
ISO 11 Physical and Environmental Security	Failed Physical Physical Access Overview Successful Physical Physical Access Overview	Failed Building Physical Access Activity Summary Failed User Physical Access Activity Summary Successful Building Physical Access Activity Summary Successful User Physical Access Activity Summary

Category	Dashboards	Reports
ISO 12 Operations Security	Administrative Login Overview	Antivirus Stopped or Paused
	Application Vulnerabilities Overview	Audit Log Cleared
	Failed Login Overview	Database Configuration Changes
	Failed Login Relationship	Database Vulnerabilities
	Firewall Configuration Changes	Failed Administrative Login Summary
	Malware Overview	Failed Antivirus Updates
	Successful Login Overview	Failed Login by SOX Asset
	Unpatched Systems	Failed Login Summary
	Vulnerability Overview	Firewall Configuration Changes
		High Risk Vulnerabilities
		Malware Summary
		Network Device Configuration Changes
		Overflow Vulnerabilities
		SQL Injection Vulnerabilities
		Successful Administrative Login Summary
		Successful Login by SOX Asset
		Unpatched Systems
		Vulnerability Summary by CVE ID
		Vulnerability Summary by SOX Asset
		Vulnerability Summary on SOX Environment
		XSRF Vulnerabilities
		XSS Vulnerabilities
ISO 13 Communications Security	DoS Activity	Covert Channel Activity
	Firewall Blocked Events	DoS Attacks Summary
		Firewall Blocked Events

Category	Dashboards	Reports
ISO 16 Information Security Incident Management	High Risk Events Overview MITRE ATT&CK Overview Reconnaissance Activity Threat Overview Threat Relationship	High Risk Events Summary MITRE ATT&CK Summary by MITRE Technique MITRE ATT&CK Summary by SOX Asset Reconnaissance Summary Threats Summary
ISO 17 Information Security Aspects of Business Continuity Management	n/a	Asset Shutdown Summary
ISO 18 Compliance	Information Disclosure Vulnerabilities Organization Information Leaks Personal Information Leakage Overview	Information Disclosure Vulnerabilities Organization Information Leaks Summary Personal Information Leakage Summary

Sarbanes-Oxley Executive Summary

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **Executive Summary**.

This category is relevant to all ISO 27002:2013 controls. To assess your enterprise's compliance with this requirement, use the following dashboards:

Dashboards	Reports
Control Overview Controls Risk Score Overview Executive Cyber Threat Overview	n/a

Control Overview

Used as a drill-down dashboard by the Controls Risk Score Overview dashboard.

Controls Risk Score Overview

Provides an overview of ISO 27002:2013 controls based on correlation events reported from ESM.

Executive Cyber Threat Overview

Provides a cyber threat overview for executives. The dashboard shows the top 5:

- Vulnerabilities

- MITRE ATT&CK techniques

- ArcSight categorized attacks

- Attacked assets

5 – Information Security Policies

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 5 Information Security Policies**.

To assess your enterprise's compliance with this requirement, use the following dashboard and report:

Dashboards	Reports
Policy Violations Overview	Policy Violations

Policy Violations Overview

Provides an overview of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

Policy Violations

Provides a summary of policy violation events that involve Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 5.1.2.

6 – Organization of Information Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 6 Organization of Information Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
VPN Connection Overview Wireless Attacks and Suspicious Activity	Outbound Communication from Development to Production Environment Outbound Communication from Production to Development Environment VPN Connection Summary Wireless Attacks and Suspicious Activity

VPN Connection Overview

Provides an overview of VPN connection activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this dashboard, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides an overview of wireless attacks and suspicious activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

Outbound Communication from Development to Production Environment

Provides a summary of outbound communication events from development to production environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXDevelopment` and `isDestinationZoneSOXProduction` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Outbound Communication from Production to Development Environment

Provides a summary of outbound communication events from production to development environments involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.1.2.

Before using this report, ensure that variables `isSourceZoneSOXProduction` and `isDestinationZoneSOXDevelopment` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

VPN Connection Summary

Provides a summary about VPN connection events which involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.2.

Before using this report, ensure that variables `isAgentZoneSOX` and `isAgentAddressSOX` are defined in the SOX logical model. For more information, see the *Solutions Guide for ArcSight Insight Compliance Package for SOX*.

Wireless Attacks and Suspicious Activity

Provides a summary of wireless attack and suspicious activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 6.2.1.

7 – Human Resource Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 7 Human Resource Security**.

Activity by User

Provides an overview of activity by specific users involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 7.1.1, 7.2.3 , and 7.3.1.

8 – Asset Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 8 Asset Management**.

Removable Media Activity

Provides an overview of removable media activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 8.3.1.

9 – Access Control

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **SOX Reports** > **ISO 9 Access Control**.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	Account Creations
	Account Deletions
	Account Lockouts by System
	Account Lockouts by User
	Insecure Ports
	Insecure Services
	Password Policy Changes
	Password Weaknesses
	User Group Account Creations
	User Group Account Deletions

Account Creations

Provides a summary of account creation activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Deletions

Provides a summary of account deletion activity events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by System

Provides a summary of account lockout activity events by system involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Account Lockouts by User

Provides a summary of account lockout activity events by user involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

Insecure Ports

Provides a summary of insecure ports that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Insecure Services

Provides a summary of insecure services that are involved in communication with Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Password Policy Changes

Provides a summary of password policy change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

Password Weaknesses

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.4.3.

User Group Account Creations

Provides a summary of user group account creation events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

User Group Account Deletions

Provides a summary of user group account deletion events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 9.2.1.

10 – Cryptography

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 10 Cryptography**.

To assess your enterprise's compliance with this requirement, use the following reports:

Dashboards	Reports
n/a	SSH Vulnerabilities
	SSL or TLS Vulnerabilities
	VPN Vulnerabilities

SSH Vulnerabilities

Provides a summary of SSH vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

SSL or TLS Vulnerabilities

Provides a summary of SSL or TLS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

VPN Vulnerabilities

Provides a summary of VPN vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 10.1.1.

11 – Physical and Environmental Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 11 Physical and Environmental Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Failed Physical Access Overview	Failed Building Physical Access Activity Summary
Successful Physical Access Overview	Failed User Physical Access Activity Summary
	Successful Building Physical Access Activity Summary
	Successful User Physical Access Activity Summary

Failed Physical Access Overview

Provides an overview of failed physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Successful Physical Access Overview

Provides an overview of successful physical access activity events, relevant to ISO 27002:2013 Control 11.1.2.

Failed Building Physical Access Activity Summary

Provides a summary of failed physical access activity events by building, relevant to ISO27002:2013 control 11.1.2.

Failed User Physical Access Activity Summary

Provides a summary of failed physical access activity events by user, relevant to
ISO27002:2013 control 11.1.2.

Successful Building Physical Access Activity Summary

Provides a summary of successful physical access activity events by building, relevant to
ISO27002:2013 control 11.1.2.

Successful User Physical Access Activity Summary

Provides a summary of successful physical access activity events by user, relevant to
ISO27002:2013 control 11.1.2.

12 – Operations Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** >
ISO 27002 > *Dashboards* or *Reports* > **ISO 12 Operations Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards
and reports:

Dashboards	Reports
Administrative Login Overview	Antivirus Stopped or Paused
Application Vulnerabilities Overview	Audit Log Cleared
Failed Login Overview	Database Configuration Changes
Failed Login Relationship	Database Vulnerabilities
Firewall Configuration Changes	Failed Administrative Login Summary
Malware Overview	Failed Antivirus Updates
Successful Login Overview	Failed Login by SOX Asset
Unpatched Systems	Failed Login Summary
Vulnerability Overview	Firewall Configuration Changes
	High Risk Vulnerabilities
	Malware Summary
	Network Device Configuration Changes
	Overflow Vulnerabilities
	SQL Injection Vulnerabilities
	Successful Administrative Login Summary
	Successful Login by SOX Asset
	Unpatched Systems
	Vulnerability Summary by CVE ID
	Vulnerability Summary by SOX Asset
	Vulnerability Summary on SOX Environment
	XSRF Vulnerabilities
	XSS Vulnerabilities

Administrative Login Overview

Provides an overview of administrative login activity, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Application Vulnerabilities Overview

Provides an overview of the following application vulnerabilities, relevant to ISO 27002:2013 Control 12.6.1:

- SQL injection

- XSS

- XSRF

- Overflow

Failed Login Overview

Provides an overview of failed login activity, relevant to ISO 27002:2013 Control 12.4.1.

Failed Login Relationship

Based on ArcSight categorization, provides an overview of failed login relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides an overview of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

Malware Overview

Provides an overview of malware activity, relevant to ISO 27002:2013 Control 12.2.1.

Successful Login Overview

Provides an overview of successful login activity, relevant to ISO 27002:2013 Control 12.4.1.

Unpatched Systems

Provides an overview of missing security patches on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Overview

Provides an overview of vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Antivirus Stopped or Paused

Provides a summary of antivirus services that were stopped or paused, relevant to ISO 27002:20213 Control 12.4.1.

Audit Log Cleared

Provides a summary of audit log cleared events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.2.

Database Configuration Changes

Provides a summary of database configuration changes, relevant to ISO 27002:2013 Control 12.1.2.

Database Vulnerabilities

Provides a summary of database vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Failed Administrative Login Summary

Provides a summary of failed administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Failed Antivirus Updates

Provides a summary of failed antivirus updates, relevant to ISO 27002:20213 Control 12.4.1.

Failed Login by SOX Asset

Provides a summary of failed logins detected on specific SOX assets , relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Failed Login Summary

Provides a summary of failed login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.1.

Firewall Configuration Changes

Provides a summary of firewall configuration change events, relevant to ISO 27002:2013 Control 12.1.2.

High Risk Vulnerabilities

Provides a summary of high-risk vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Malware Summary

Provides a summary of malware events on Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.2.1.

Network Device Configuration Changes

Provides a summary of network device configuration change events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.1.2.

Overflow Vulnerabilities

Provides a summary of overflow vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

SQL Injection Vulnerabilities

Provides a summary of SQL vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

Successful Administrative Login Summary

Provides a summary of successful administrative login events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.4.3.

To define administrative accounts, use the worksheet condition of this dashboard. Use lowercase to define the accounts. For example, add the user "Administrator" as "administrator."

Successful Login by SOX Asset

Provides a summary of successful logins detected on specific SOX assets, relevant to ISO 27002:2013 control 12.4.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Unpatched Systems

Provides a summary of missing security patches involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.5.1.

Vulnerability Summary by CVE ID

Provides a summary of vulnerabilities detected on SOX environments by specific CVE ID, relevant to ISO 2700:2013 Control 12.6.1.

When you run this report, specify the CVE ID in lowercase.

Vulnerability Summary by SOX Asset

Provides a summary of vulnerabilities detected on specific SOX assets, relevant to ISO 27002:2013 Control 12.6.1.

When you run this report, specify the asset (host name, IP address, or MAC address) in lowercase.

Vulnerability Summary on SOX Environment

Provides a summary of vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSRF Vulnerabilities

Provides a summary of XSRF vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

XSS Vulnerabilities

Provides a summary of XSS vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 12.6.1.

13 – Communications Security

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 13 Communications Security**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
DoS Activity	Covert Channel Activity
Firewall Blocked Events	DoS Attacks Summary
	Firewall Blocked Events

DoS Activity

Based on ArcSight categorization, provides an overview of DoS activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides an overview of blocked firewall events, relevant to ISO 27002:2013 Control 13.2.1.

Covert Channel Activity

Displays covert channel activities, relevant to ISO 27002:2013 Control 13.2.1.

DoS Attacks Summary

Provides a summary of events that indicate DoS activity, relevant to ISO 27002:2013 Control 13.2.3.

Firewall Blocked Events

Provides a summary of blocked firewall events, relevant to ISO27002:2013 control 13.2.1

16 – Information Security Incident Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 16 Information Security Incident Management**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
High Risk Events Overview	High Risk Events Summary
MITRE ATT&CK Overview	MITRE ATT&CK Summary by MITRE Technique
Reconnaissance Activity	MITRE ATT&CK Summary by SOX Asset
Threat Overview	Reconnaissance Summary
Threat Relationship	Threats Summary

High Risk Events Overview

Provides an overview of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Overview

Provides an overview of MITRE ATT&CK events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Activity

Based on ArcSight categorization, provides an overview of reconnaissance activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Overview

Based on ArcSight categorization, provides an overview of threat activity involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threat Relationship

Based on ArcSight categorization, provides overview of threat relationships involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

High Risk Events Summary

Provides a summary of high-risk events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by MITRE Technique

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by MITRE technique, relevant to ISO 27002:2013 Control 16.1.2.

MITRE ATT&CK Summary by SOX Asset

Provides a summary of MITRE ATT&CK events involving Sarbanes Oxley systems by target asset, relevant to ISO 27002:2013 Control 16.1.2.

Reconnaissance Summary

Provides a summary of reconnaissance events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

Threats Summary

Provides a summary of threat events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 16.1.2.

17 – Information Security Aspects of Business Continuity Management

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > **Reports** > **ISO 17 Information Security Aspects of Business Continuity Management**.

Asset Shutdown Summary

Provides a summary of asset shutdown events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Control 17.1.3.

18 – Compliance

Select **Reports** > **Portal** > **Repository** > **Data Compliance Content** > **Sarbanes Oxley** > **ISO 27002** > *Dashboards* or *Reports* > **ISO 18 Compliance**.

To assess your enterprise's compliance with this requirement, use the following dashboards and reports:

Dashboards	Reports
Information Disclosure Vulnerabilities	Information Disclosure Vulnerabilities
Organization Information Leaks	Organization Information Leaks Summary
Personal Information Leakage Overview	Personal Information Leakage Summary

Information Disclosure Vulnerabilities

Provides an overview of information disclosure vulnerability events involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks

Based on ArcSight categorization, provides an overview of information leakage activity (for example, company data), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Overview

Based on ArcSight categorization, provides an overview of personal information leakage activity, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Information Disclosure Vulnerabilities - Dashboard

Provides a summary of information disclosure vulnerabilities involving Sarbanes Oxley systems, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Organization Information Leaks Summary - Dashboard

Provides a summary of information leakage events (for example, company data leaks), relevant to ISO 27002:2013 Controls 18.1.3, 13.2.4.

Personal Information Leakage Summary - Dashboard

Provides a summary of personal information leakage events, relevant to ISO 27002:2013 Controls 18.1.4, 13.2.4.

Managing and Importing 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 ArcSight 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 the ArcSight Database 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.

Managing Your Stored 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

You 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. Higher volumes of event data, require more storage space. The **storage utilization** column displays the amount of storage utilized.

The **query filter** enables you to associate a storage group with specific compliance requirements, business needs, or search activities. Your specified query filters 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, the event gets sent to the *Default Storage Group*. You cannot change the name, query, or rank of this built-in group.

> By default, the maximum value for retaining events in the *Default Storage Group* is 12 months. However, the license for your deployed product might require a lower maximum value, such as 30 days. For more information about how deployed products affect data retention policies in a non-SaaS environment, see "Understanding License Keys" in the *Administrator's Guide for ArcSight Platform*.

The **Apply Changes to System** option at the top of the Storage Groups page indicates that one or more groups have been modified but the changes need to be applied.

- Create a Storage Group
- Direct Events to the Correct Storage Group

Create a Storage Group

You can have up to **10 storage groups**, including the provided *Default Storage Group*.

1. Select **Configuration** > **Storage**.

2. Click the **add** icon **+**.

3. Enter a name for the storage group.

   > ⚠ **CAUTION:** You cannot change the name after you create the group.

   > The name cannot include special characters other than a hyphen (-).

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. Click **Save**.

8. Apply your changes.

Direct Events to the Correct Storage Group

For efficient data retrieval, the system matches each incoming event with the query filter for a 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, the system **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 the system assigns the event to the group that is ranked 3. If an event does not match any of the active filters, the system sends the event to the *Default Storage Group*.

You can change the ranking of storage groups to ensure that the system places events in the best location.

1. Select **Configuration** > **Storage**.

2. From the **Storage Information** table, drag each storage group up or down to the preferred priority position.

   The system always places the *Default Storage Group* in the lowest ranked position.

Activate and Deactivate Storage Groups

The application allows you to have up to **10 storage groups**, including the provided *Default Storage Group*. To deactivate to prevent new events from being sent to the group, change a storage group's status. For example, you might no longer need a particular storage group or find that you have changed the filters and functionality of that group from its original purpose. Rather than continuing to modify an existing group, you can deactivate it. Alternatively, you might want to activate a storage group only during certain periods of time.

Although you deactivate a group, the deletion settings for that group remain in effect.

1. Select **Configuration** > **Storage**.

2. Select the storage group that you want to activate or deactivate.

3. To edit the group's settings, click the ✏ icon.

4. For **Group Status**, slide the indicator left or right.

   Activated groups display a status of **Active**.

5. Click **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
- Apply Your Changes to a Storage Group

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. Click the **pencil** icon ✎.

4. For **Group Status**, slide the indicator left or right.

5. Activated groups will display a status of **Active**.

6. Click **Save**.

7. 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, the system 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, the ArcSight Database 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, the database begins deleting all data older than three months.

- While changes are being applied, you cannot create or modify a storage group.

Use Storage Group Queries in a Search

Search allows you to specify the storage group in which you want to search events. 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.

Configure Retention Policies for Your Data

Events are stored in their assigned storage groups 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 your system to purge certain data, such as DNS logs that are older than 24 months.

When setting the policies for storage group retention and disk space utilization, do not allow your disk space utilization to increase above 90%. Running out of disk space can reduce the performance of searches due to increasing fragmentation. If such a situation continues to where there is no space left, then the database cannot ingest new data.

Delete Old Data from Storage Groups

Events are stored in their assigned storage groups 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, the data retention policy for your organization might expect data older than 24 months to be purged. This process **deletes data from the database**.

The system 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, when you want old events to be deleted.

   > By default, the maximum value for retaining events in the Default Storage Group is 12 months. However, the license for your deployed product might require a lower maximum value, such as one month. With a Log Management and Compliance (Recon) license, you can set the value to "-1" which enables the storage group to **Never Expire** for a long-term storage option.

Ensure that your retention policy takes into consideration the maximum size of your storage groups and database. Also, consider that, in deleting events, the policy might affect results of an Event Integrity Check.

3. Click **Save**.

4. Apply your changes.

Manage Retention Policies for Imported Logger Data

> ⚠️ You can have up to 10 storage groups overall (including both groups created in the ArcSight Database and those migrated from Logger). Exceeding this quantity will likely affect the performance.

To manage the storage and expiration of the recently imported data from Logger, the system automatically enables the retention policy for the Logger event data. You do not need to manually direct events to a certain storage group and implement additional retention policies, but rather take advantage of the same storage rules already set in Logger.

You can update and review the retention policy strictly from the Logger interface. However, changes made to the retention policy after the archive migration has been started won't be reflected on the archives imported to the ArcSight Database.

> 🏠 For more information about retention policies for event data, see "Storage" in the *Administrator's Guide to ArcSight Logger*.

For a non-SaaS environment

As part of the metadata migration, the tool brings in the Storage Groups and their retention information. Because in Logger the retention settings are based on days, the tool converts them to months and rounds it up as to comply with the format used by the ArcSight Database. If the Maximum Archives Age value was set to -1 for a Storage Group in Logger (meaning a disabled retention policy), the retention process for it will also be disabled in ArcSight Platform.

For a SaaS environment

When you migrate Logger data to a SaaS environment, the system temporarily stores data in an AWS S3 bucket. For successfully migrated data, the system deletes the temporary files stored in the bucket after a month.

For data that hasn't been imported, the temporary files will be deleted from the bucket based on the ArcSight license purchased by your organization.

The retention period for data imported to the ArcSight Database will be either the **Storage Group Retention** value (from Logger) or the one established by the ArcSight license, depending on which one is lower.

For more information about preparing for data migration, see Installing the AWS Command Line Interface in Each Logger in the *ArcSight SaaS Quick Start for Administrator's* guide.

Managing the Quality of Your Data

Requires the Log Management and Compliance service in ArcSight SIEM as a Service or the ArcSight Recon capability .

Select **Insights** > **Data Quality**.

The **Data Quality Dashboard** provides detailed information about the gap between Device Receipt Time from the raw event itself versus the Normalized Event Time and Database Receipt Time. Data Quality Dashboard identifies the sources that cause issues with the data. Based on the information analyzed through the Data Quality Dashboard, you can accurately mitigate the problem. This feature also provides history of your data over time.

- Understanding the Data Quality Insights
- Understanding How Data Quality is Calculated
- Analyzing Data Quality

Understanding the Data Quality Insights

Content in the Data Quality Dashboard is divided into the following categories that represent how big the gaps are among Database Receipt Time (dBRT), Device Receipt Time (DRT), and Normalized Event Time (NET):

- Active Events
- Future Events
- Past Events

Active Events

Indicates that your events have a timestamp within the database's active time frame where `NET - DRT = 0`. The Data Quality Dashboard presents active events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Within 1 Minute	Data received in the ArcSight database with less than a one-minute gap	`dBRT- DRT = values between -60000 and 60000` milliseconds
Hour Ahead	Data received between one minute and an hour before DRT	`dBRT- DRT = a value between -3600000 and -60001` milliseconds
Hour Behind	Data received between one minute and an hour after DRT	`dBRT- DRT = a value between 60001 and 3600000` milliseconds
Day Ahead	Data received between one and 24 hours before DRT	`dBRT- DRT = a value between -86400000 and -3600001` milliseconds
Day Behind	Data received between one and 24 hours after DRT	`dBRT - DRT = a value between 3600001 and 86400000` milliseconds
Week Behind	Data received between one day and one week after DRT	`dBRT - DRT = a value between 86400001 and 604800000` milliseconds

Future Events

Indicates that your events have a future timestamp where $NET - DRT < 0$. The Data Quality Dashboard presents future events in sub-categories based on the following time gaps between DRT and dBRT:

Sub-category	Description	Formula
Week Ahead	Data received between one and seven days before DRT	`dBRT - DRT = a value between -604800000 and -86400001` milliseconds
Far Future	Data received more than a week before DRT	`dBRT - DRT < -604800001` milliseconds

The **Far Future** critical category helps identify events that fall well outside the most accepted variance range.

Past Events

Indicates that events have a past timestamp where $NET - DRT > 0$. The Data Quality Dashboard presents past events in a sub-category based on the following time gap between DRT and dBRT:

Sub-category	Description	Formula
Distant Past	Data received more than a week after DRT	`dBRT - DRT > -604800001` milliseconds

The **Distant Past** critical category helps identify events that fall well outside the most accepted variance range.

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 ArcSight Database was installed or upgraded.

During a fresh installation, the process creates a new table to store Data Quality over time, with source information. The feature schedules the aggregation process at the tenth minute of every hour. For example, if a fresh install or upgrade was completed at 9:15:00 AM, the aggregation would be scheduled to execute at 10:10:00 AM and 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.

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 Custom Range and Quick Ranges. By default, the Dashboard displays data per the **Last week** setting. If the Chron Job has not been run yet, the charts would display no data.

Data-Time series

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 12 Data Categories. *Far Future* is the default selection.

- **Top 10 Agents from Future Events**

  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, host name, and number of events of each source, hover over each donut piece. If you click a donut piece, the Hourly Event Volume chart displays more values.

- **Hourly Event Volume**

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

Importing Event Data From Logger

If you have ArcSight Logger deployed, you can import event data from Logger into the ArcSight Database to enable you to search on that data from within ArcSight Platform. To do so, the process requires you to first import the Logger event metadata, then Logger event archives into the Database. After the system successfully imports a Logger archive file, the events in that archive file will be available in the Database. You can gradually import the Logger archive files as needed.

> ✓ **NOTE**: Depending on your version of ArcSight Platform (SaaS or non-SaaS), this feature will follow a different procedure. Ensure that you select the right one for your environment.

Importing Logger Data to the ArcSight Database (SaaS)

Applies only for the ArcSight SaaS environment.

> ⚠ This process can be started only after the metadata migration process has been started from at least one of the available Logger(s)

If you have ArcSight Logger deployed in your network infrastructure, you can search Logger event data collected over time. To do so, you must import the events stored in the Logger archives to the ArcSight Database. This process requires you to first import the event metadata, then the event data. Before you begin searching through Logger data, ensure that the data migrations have completed. The system stores the imported archives according to the retention policies established in Logger.

1. Verify that you have imported metadata from at least one available Logger.

   For more information, see "Importing Logger Data to the ArcSight Database" in the *ArcSight SaaS Quick Start for Administrator's* guide.

2. Select **Configuration > Import Logger Data > Data Import**.

3. In the **Select the Logger for Data Import** menu, select the Logger from which you want to import the data.

   For more information about Logger aliases, see "Managing the S3 Bucket" in the *ArcSight SaaS Quick Start for Administrator's* guide.

   For the selected Logger, the system displays a list of the archives stored. You can find this in a table under the **Displaying x results** label. For each archive, the table displays the following information. To filter the displayed information, you can enter search for values within each column.

   Archive Name

   Represents the name of the archive, as assigned in Logger. For more information, see "Archiving Events" in the *Administrator's Guide to ArcSight Logger*.

   Day

   Represents the day of the month that Logger generated the archive. Values are 01 to 31 (depending on the month).

   Month

   Represents the month that Logger generated the archive. Values are 01 to 12.

   Year

   Represents the year that Logger generated the archive. Values are displayed in a 4-digit format.

   Storage Group

   Represents the name of the Logger associated with the archive.

   Data Files

   Displays the number of files contained in the archive, as well as indicating the number of the files that have been correctly imported (files without missing data). For example, 2/3 means there are 3 files in the archive, and 2 of them were imported correctly.

   Import Status

   Indicates the status of the migration of the archive.

   The import process follows this order: **Not imported** > **Pending Import**> **Importing**. Note that the Pending Import state can take up to 5 minutes to complete the archive analysis. The result of the importing process can be either **Imported** or **Import Failed**.
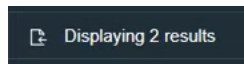
Import Date

> Represents the date that the archive was imported. If the import has not been performed, it will appear as "---".

Archive Size

> Show the size of the archive in gigabytes.

4. Check the box to the left of each archive that you want to enable for import.

   After you select a Logger, the system displays the **Import** button will appear to the left of **Displaying x results**:

5. To start importing the selected archives, click **Import**.

   The system updates the import state of each archive as the process proceeds.

   > Only archives with an import state of **Not Imported** have a check box and are available for import.
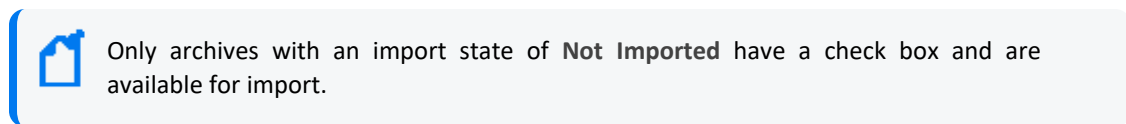
6. (Optional) To update the list of archives contained in the Logger, click **Refresh** to the right of the Search box.

7. (Optional) After the system has successfully imported Logger event data, you can search for the Logger events.

Importing Logger Data to the ArcSight Database (non-SaaS)

Does not apply in a SaaS environment.

> ⚠ The procedure and steps described in this section have been tested with Logger and ArcSight Platform installed on two different machines
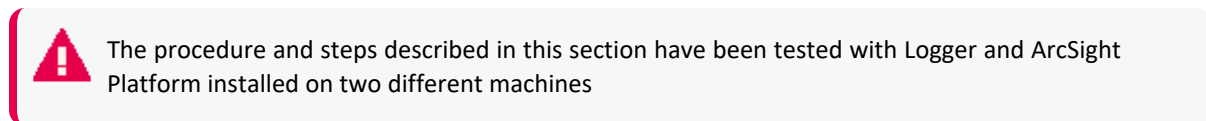
This section guides you through the process of importing the Logger metadata and then its corresponding archived events to the ArcSight Database. Before you start searching the imported Logger archived events, ensure that the data migrations have completed according to the procedures in "Migrating Logger Data to the ArcSight Database" in the *Administrator's Guide to ArcSight Platform 23.3*.

To start the procedure, please follow the Checklist: Migrating Logger Data.

Checklist: Migrating Logger Data

Does not apply in the ArcSight SaaS environment.

Use the following checklist to migrate event data from Logger. You must perform the tasks in the listed order.

	Task	See
☐	1. Ensure that you have read the considerations and can comply with the prerequisites for importing Logger data	Prerequisites and Considerations for Importing Logger Data in the *Administrator's Guide to ArcSight Platform 23.3*
☐	2. Import the Logger event metadata	Import Metadata for Logger Events
☐	3. (Optional) Shut down the Logger instance after successfully importing the metadata	Removing a Logger after Its Data Is Copied to the ArcSight Database
☐	4. Import the Logger event data that you want to search	Import Logger Events

Import Metadata for Logger Events

Does not apply in a SaaS environment.

Select **Configuration > Import Logger Data > Logger Metadata Import**.

> ⚠ **This topic applies only to Logger processes soon-to-be shut down.**

Logger metadata refers to the information that is stored in the Logger `postgresql` database, which is needed to read the events from the Logger archive files for each storage group.

You import the metadata once for each Logger whose processes are soon to be shutdown. Complete the following activities:

- Register a Logger
- Import the Metadata
- Update the Logger Registration

Register a Logger

Applies only if you have not previously registered the Logger from which you will import data

Before importing the metadata, make sure to add the Logger details for the import process.

1. In ArcSight Platform, select **Configuration > Import Logger Data > Logger Metadata Import**.

2. Click the **+** icon.

3. Add the Logger details such as:

   a. **Host**: Logger IP address or host name
      For example, 12.345.67.890 or `logger6.extremelyfocused.com`

   b. **Host Username**: OS username

   c. **Host Password**: OS password

4. Click **Save**. Otherwise, click **Cancel**.

> **Note:** You can remove Logger registration if no data has been imported. To delete the Logger registration, click the delete icon (trash can).

Import the Metadata

> **Note:** It's recommended that you perform the following steps before the actual metadata import:
> - Stop all Logger event ingestion
> - Switch connectors to send events to the ArcSight Database
> - Archive all the existing events in Logger before importing the Logger metadata

While importing the metadata, the Logger server must be accessible at all times.

The metadata contains all the information related to accessing the events of a particular Logger. You can migrate the Logger metadata to the ArcSight Database directly from the **Logger Metadata Import** page.

> ⚠ Make sure to import the metadata before importing the Logger data as this is the first step to view and consume logger events.

1. In ArcSight Platform, select **Configuration > Import Logger Data > Logger Metadata Import**.

2. Check the box next to the Logger whose metadata will be migrated and click the **import** icon.

   A pop-up window will notify you that the Logger metadata import procedure is about to begin, making sure you have already mounted the appropriate archives on all database nodes.

At this point, you must decide whether Logger processes resume after the import of metadata is done:

- **Yes**: The Logger processes will resume after the import is finished. ArcSight Platform proceeds to import and store the metadata.

- **No**: The Logger processes will remain shut down. ArcSight Platform proceeds to import and store the metadata.

> After successfully importing the metadata and the Logger processes have been shut down, you have the option to remove or repurpose that particular Logger.

- **Cancel**: The system will not continue with the process for importing the metadata. The Logger continues in its current state.

Update the Logger Registration

Required only if user credentials for the registered Logger have changed.

If the credentials have been changed after registering a Logger, make sure to update the username and password information before importing the Logger metadata.

The Logger processes status, host username, and password can be updated after the Logger registration, but only if the metadata import process hasn't started.

These values cannot be updated after you start an import.

1. In ArcSight Platform, select **Configuration > Import Logger Data > Logger Data Import**.

2. Check the box next to the Logger host and click the pencil icon.

3. Update the values accordingly.

   Ensure that the username and password that you use match the OS credentials set in Logger.

4. Click **Save**. Otherwise, click **Cancel**.

Removing a Logger after Its Data Is Copied to the ArcSight Database

This process is optional. Does not apply in a SaaS environment.

After you have successfully imported the metadata , you have the option to remove or repurpose that particular Logger. The next phase, where you import the archived event data, does not require the Logger.

1. To ensure that the Logger will no longer receive events, reconfigure the SmartConnectors to send events to the ArcSight SaaS environment.

2. Log in to ArcSight.

   Note that your login role must have the *Logger Data Migration* permission.

3. Select **Configuration** > **Import Logger Data** > **Data Import**.

4. Verify that all archives are listed and thus ready for import to the ArcSight Database.

   We recommend that you check the listed archives to ensure that you have copied all desired metadata from each Logger.

5. Shut down the Logger process.

   You can now repurpose the Logger host system.

Import Logger Events

Does not apply in a SaaS environment.

Select **Configuration** > **Import Logger Data** > **Logger Data Import**.

This option will allow you to bring events from a Logger instance to the ArcSight Database and perform searches on them. Since this process consumes both time and resources, consider importing only events in necessary time ranges.

> ⚠️ Before you can migrate Logger data, you must import the metadata that defines it.

- Import Archived Events
- Review Migration Details
- Resume an Incomplete Migration
- Delete Incomplete or Failed Migrations

Import Archived Events

Before importing Archived Events, ensure that you have performed the process from the Logger side first. For more information, see "Migrating Logger Data to the ArcSight Database" in the *Administrator's Guide for ArcSight Platform*.

1. Select **Configuration** > **Import Logger Data** > **Logger Data Import**.

2. Click **+**.

3. Select the Logger host of your preference.

   You can choose only one host at a time.

4. Specify the time range that you want to import, following these considerations:

- The time range is based on receipt time.

  > Convert the time range you wish to search through from browser time/selected time zone to UTC.
  >
  > That way, once the data is imported, you can search through it using the original browser time/selected time zone.

- The migration only allows you to migrate a minimum time range of 1 day.

- Specify a date in the past. You cannot import data for future dates as it will import no events and will cause issues when you try to import new data again.

- Overlapping dates will cause an error message. If this is not the first import of this Logger instance, ensure to select a time range different than the one already imported.

  > Select a data-time range different than the one already imported. To confirm the host's start and end dates already available in the ArcSight Database, see how to verify the migration table in Review Migration Details

5. Click **Import**.

6. To check the import progress, view the **Import Status** column.

   The import will take a considerable amount of time, based on the quantity of events that are present in the time range selected.

7. (Optional) If the import is interrupted, you can attempt to resume the process.

   Alternatively, you can delete an incomplete migration.

Review Migration Details

The migrations table will display the most relevant information of all the imports executed. For each migration, the system registers the following details:

Logger Host
  Represents the Logger IP address or host name. For example, `12.345.67.890` or `logger6.extremelyfocused.com`.

Data Start Date
  Indicates the absolute date of the earliest possible event.

Data End Date
  Indicates the absolute date of the latest possible event.

Import Date

Indicates the migration date and time displayed in the ArcSight Database timezone.

Import Status

Indicates the status of the import process.

Ensure that you comply with the prerequisites before importing data. For more information, see Prerequisites and Considerations for Importing Logger Data in the *Administrator's Guide to ArcSight Platform 23.3*.

- **Initialized**: The verification of the archives corresponding to the requested time range is being performed.

- **In progress**: Import is still in progress. Archived events are being extracted, read and sent to the ArcSight Database.

- **Complete**: Successfully imported the data.

- **Failed**: The archives are inaccessible, which can be caused by:

  ○ An unresponsive mount

  ○ A network connectivity issue

  ○ A user who doesn't have the correct access permissions

  ○ Data that couldn't be uncompressed, etc

Event Count

Indicates the number of events migrated. This number increases automatically as the process continues.

Logger Host User Name

Indicates the OS username associated with the Logger host.

Data Import ID

Represents the unique identifier for the event migration. You must have this value to delete a migration.

To review details about the executed migration, see the logs in the `opt/vertica/udfs/datamigration/logs/` directory.

After events have been imported, either Logger or ArcSight Platform will manage the retention policy depending on the state of the Logger processes.

Resume an Incomplete Migration

A migration might be interrupted if access to the mount or data file is affected in any way during the process: an unresponsive mount, a network connectivity issue, a user who doesn't have the correct access permissions, data that couldn't be uncompressed, etc.

An **Incomplete** migration can be resumed. The process starts from the last point of migration so you do not lose the data previously migrated.

1. Select the migrations that you want to resume.

2. Click ⊡.

A migration that continues to appear as **incomplete** after it has been resumed at least once, might indicate the data cannot be migrated because of corruption issues.

Check the logs for any related messages, and contact support to help finish the migration.

Delete Incomplete or Failed Migrations

It's possible that a migration might fail to complete. For example, the status is **Failed** or indicates that the migration is **Complete** but it contains no events. In these types of scenarios, you can delete the migration, then try again.

1. Select the migrations that you want to delete.

2. Click 🗑.

Appendices

The appendices in this guide provide additional information or guidance for using the features and functions for this product.

Mapping Database Names to their Appropriate Search Fields

When creating a fieldset, Search displays the coding-style name for the fields instead of the human-readable names that you see when creating a query. For example, in a query you can enter or select `Agent Address`. However, in the fieldsets selection, this same field appears as `agentAddressBin`. This issue also occurs when you're adding queries to a report.

The following tables provide the coding-style names that appear in the fieldset and report configurations, so that you can easily map them to their human-readable names.

Agent Fields

Substitute the following labels in the agent category:

For the field that you want to add...	You should choose...
Agent Address	agentAddressBin
Agent DNS Domain	agentDnsDomain
Agent Hostname	agentHostName
Agent ID	agentId
Agent Mac Address	agentMacAddressBin
Agent NT Domain	agentNtDomain
Agent Receipt Time	agentReceiptTime
Agent Severity	agentSeverity
Agent Timezone	agentTimeZone
Agent Translated Address	agentTranslatedAddressBin
Agent Translated Zone External ID	agentTranslatedZoneExternalID

Agent Translated Zone URI	agentTranslatedZoneURI
Agent Type	agentType
Agent Version	agentVersion
Agent Zone External ID	agentZoneExternalID
Agent Zone URI	agentZoneURI

Category Fields

Substitute the following labels in the category:

Category Behavior	categoryBehavior
Category Device Group	categoryDeviceGroup
Category Device Type	categoryDeviceType
Category Object	categoryObject
Category Outcome	categoryOutcome
Category Significance	categorySignificance
Category Technique	categoryTechnique
Version	version

Correlation Fields

Substitute the following labels in the `correlation` category:

Substitute the following labels in the correlation category:	You should choose...
Base Event Ids	correlated_event_id
Correlated Event Id	generatorURI
Generator External ID	generatorExternalID
Generator URI	base_event_ids
Priority	priority

Destination Fields

Substitute the following labels in the `destination` category:

For the field that you want to add...	You should choose...
Destination Address	destinationAddressBin

Destination DNS Domain	destinationDnsDomain
Destination Geo Country Code	destinationGeoCountryCod
Destination Geo Latitude	destinationGeoLatitude
Destination Geo Longitude	destinationGeoLongitude
Destination Geo Postal Code	destinationGeoPostalCode
Destination Geo Region Code	destinationGeoRegionCode
Destination Geolocation Info	destinationGeoLocationInfo
Destination Hostname	destinationHostName
Destination Mac Address	destinationMacAddressBin
Destination NT Domain	destinationNtDomain
Destination Port	destinationPort
Destination Process ID	destinationProcessId
Destination Process Name	destinationProcessName
Destination Service Name	destinationServiceName
Destination Translated Address	destinationTranslatedAddressBin
Destination Translated Port	destinationTranslatedPort
Destination Translated Zone External ID	destinationTranslatedZoneExternalID
Destination Translated Zone URI	destinationTranslatedZoneURI
Destination User ID	destinationUserId
Destination User Privileges	destinationUser Privileges
Destination Username	destinationUserName
Destination Zone External ID	destinationZoneExternalID
Destination Zone URI	destinationZoneURI

Device Fields

Substitute the following labels in the device category:

For the field that you want to add...	You should choose...
Device Action	deviceAction
Device Event Class ID	deviceEventClassId
Device Address	deviceAddressBin
Device Asset ID	deviceAssetID

Device Direction	deviceDirection
Device DNS Domain	deviceDnsDomain
Device Domain	deviceDomain
Device Event Category	deviceEventCategory
Device Inbound Interface	deviceInboundInterface
Device Event Class ID	deviceEventClassId
Device External ID	deviceExternalId
Device Facility Hostname	deviceFacility
Device Hostname	deviceHostName
Device Mac Address	deviceMacAddressBin
Device NT Domain	deviceNtDomain
Device Outbound Interface	deviceOutboundInterface
Device Process ID	deviceProcessId
Device Process Name	deviceProcessName
Device Product	deviceProduct
Device Receipt Time	deviceReceiptTime
Device Severity	deviceSeverity
Device Timezone	deviceTimeZone
Device Translated Address	deviceTranslatedAddressBin
Device Translated Zone External ID	deviceTranslatedZoneExternalID
Device Translated Zone URI	deviceTranslatedZoneURI
Device Version	deviceVendor
Device Version	deviceVersion
Device Zone External ID	deviceZoneExternalID
Device Zone URI	deviceZoneURI
Normalized Event Time	normalizedEventTime

Device Custom Fields

Substitute the following labels in the `device custom` category:

For the field that you want to add...	You should choose...
Device Custom Date 1	deviceCustomDate1
Device Custom Date 1 Label	deviceCustomDate1Label
Device Custom Date 2	deviceCustomDate2
Device Custom Date 2 Label	deviceCustomDate2Label
Device Custom Descriptor ID	deviceCustomDescriptorId
Device Custom Floating Point 1	deviceCustomFloatingPoint1
Device Custom Floating Point 1 Label	deviceCustomFloatingPoint1Label
Device Custom Floating Point 2	deviceCustomFloatingPoint2
Device Custom Floating Point 2 Label	deviceCustomFloatingPoint2Label
Device Custom Floating Point 3	deviceCustomFloatingPoint3
Device Custom Floating Point 3 Label	deviceCustomFloatingPoint3Label
Device Custom Floating Point 4	deviceCustomFloatingPoint4
Device Custom Floating Point 4 Label	deviceCustomFloatingPoint4Label
Device Custom Number 1	deviceCustomNumber1
Device Custom Number 1 Label	deviceCustomNumber1Label
Device Custom Number 2	deviceCustomNumber2
Device Custom Number 2 Label	deviceCustomNumber2Label
Device Custom Number 3	deviceCustomNumber3
Device Custom Number 3 Label	deviceCustomNumber3Label
Device Custom String 1	deviceCustomString1
Device Custom String 1 Label	deviceCustomString1Label
Device Custom String 2	deviceCustomString2
Device Custom String 2 Label	deviceCustomString2Label
Device Custom String 3	deviceCustomString3
Device Custom String 3 Label	deviceCustomString3Label
Device Custom String 4	deviceCustomString4
Device Custom String 4 Label	deviceCustomString4Label
Device Custom String 5	deviceCustomString5
Device Custom String 5 Label	deviceCustomString5Label
Device Custom String 6	deviceCustomString6

For the field that you want to add...	You should choose...
Device Custom String 16 Label	deviceCustomString6Label
Device CustomIPv6 Address 1	deviceCustomIPv6Address1Bin
Device CustomIPv6 Address 1 Label	deviceCustomIPv6Address1Label
Device CustomIPv6 Address 2	deviceCustomIPv6Address2Bin
Device CustomIPv6 Address 2 Label	deviceCustomIPv6Address2Label
Device CustomIPv6 Address 3	deviceCustomIPv6Address3Bin
Device CustomIPv6 Address 3 Label	deviceCustomIPv6Address3Label
Device CustomIPv6 Address 4	deviceCustomIPv6Address4Bin
Device CustomIPv6 Address 4 Label	deviceCustomIPv6Address4Label

Event Fields

Substitute the following labels in the event category:

For the field that you want to add...	You should choose...
Application Protocol	applicationProtocol
Base Event Count	baseEventCount
Bytes In	bytesIn
Bytes Out	bytesOut
Crypto Signature	cryptoSignature
Customer External ID	customeExternalID
Customer URI	customerURI
End Time	endTime
Event ID	eventId
Event Outcome	eventOutcome
External Id	externalID
Locality	locality
Message	message
Name	name
Originator	originator
Reason	reason

For the field that you want to add...	You should choose...
Start Time	startTime
Transport Protocol	transportProtocol
Type	type

Extension Fields

Substitute the following labels in the `extension` category:

For the field that you want to add...	You should choose...
Extra Fields	extraFields
Storage Group	storageGroup

File Fields

Substitute the following labels in the `file` category:

For the field that you want to add...	You should choose...
File Create Time	fileCreateTime
File Hash	fileHash
File ID	fileId
File Modification Time	fileModificationTime
File Name	fileName
File Path	filePath
File Permission	filePermission
File Size	fileSize
File Type	fileType

Flex Fields

Substitute the following labels in the `flex` category:

For the field that you want to add...	You should choose...
Flex Date 1	flexDate1
Flex Date 1 Label	flexDate1Label
Flex Number 1	flexNumber1

For the field that you want to add...	You should choose...
Flex Number 1 Label	flexNumber1Label
Flex Number 2	flexNumber2
Flex Number 2 Label	flexNumber2Label
Flex String 1	flexString1
Flex String 1 Label	flexString1Label
Flex String 2	flexString2
Flex String 2 Label	flexString2Label

OldField Fields

Substitute the following labels in the `oldfield` category:

For the field that you want to add...	You should choose...
Old File Create Time	oldFileCreateTime

Old File Fields

Substitute the following labels in the `old file` category:

For the field that you want to add...	You should choose...
Old File Hash	oldFileHash
Old File ID	oldFileId
Old File Modification Time	oldFileModificationTime
Old File Name	oldFileName
Old File Path	oldFilePath
Old File Permission	oldFilePermission
Old File Size	oldFileSize
Old File Type	oldFileType

Request Fields

Substitute the following labels in the `request` category:

For the field that you want to add...	You should choose...
Request Client Application	requestClientApplication
Request Context	requestContext
Request Cookies	requestCookies
Request Method	requestMethod
Request URL	requestUrl
Request URL FileName	requestUrlFileName
Request URL Query	requestUrlQuery

Source Fields

Substitute the following labels in the source category:

For the field that you want to add...	You should choose...
Source Address	sourceAddressBin
Source DNS Domain	sourceDnsDomain
Source Geo Country Code	sourceGeoCountryCode
Source Geo Latitude	sourceGeoLatitude
Source Geo Longitude	sourceGeoLongitude
Source Geo Postal Code	sourceGeoPostalCode
Source Geo Region Code	sourceGeoRegionCode
Source Geolocation Info	sourceGeoLocationinfo
Source Hostname	sourceHostName
Source Mac Address	sourceMacAddressBin
Source NT Domain	sourceNtDomain
Source Port	sourcePort
Source Process ID	sourceProcessId
Source Process Name	sourceProcessName
Source Service Name	sourceServiceName
Source Translated Address	sourceTranslatedAddressBin
Source Translated Port	sourceTranslatedPort
Source Translated Zone External ID	sourceTranslatedZoneExternalID
Source Translated Zone URI	sourceTranslatedZoneURI

For the field that you want to add...	You should choose...
Source User ID	sourceUserId
Source User Privileges	sourceUser Privileges
Source Username	sourceUserName
Source Zone External ID	sourceZoneExternalID
Source Zone URI	sourceZoneURI

Publication Status

Released: NOT RELEASED

Staged: Not staged

Updated: Tuesday, October 10, 2023