MICRO FOCUS

Fusion 1.5.1 in the ArcSight Platform

User’s Guide

April 2022

Copyright Notice

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

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

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

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

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

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

Contents

About This Book

This *User's Guide* provides concepts, use cases, and contextual help for the Fusion common layer of services for the ArcSight Platform, helping you with the following activity:

Intended Audience

This book provides information for individuals who need to create users, groups, and roles; create and run reports and dashboards, and use the ArcSight Dashboard. These individuals have experience using security products to analyze events, as well as creating reports and dashboards.

Additional Documentation

When you use Fusion with the ArcSight Platform or ArcSight SIEM as a Service, the documentation library includes the following resources:

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 (https://www.microfocus.com/documentation/arcsight/arcsight-saas/) for the capabilities that you can deploy in your ArcSight Platform environment

ArcSight Platform for non-SaaS environments

- *Release Notes for ArcSight Platform 22.1*, which provides an overview of the products deployed in this suite and their latest features or updates
- *Administrator Guide for ArcSight Platform 22.1*, which provides information about deploying, configuring, and maintaining the product; you deploy Fusion with these solutions
- *Technical Requirements for ArcSight Platform 22.1*, which provides information about the hardware and software requirements for installing ArcSight Platform
- User Guides and Release Notes (https://www.microfocus.com/documentation/arcsight/arcsight-platform-22.1/) for the capabilities that you can deploy in your ArcSight Platform environment

For the most recent version of this guide and other ArcSight documentation resources, visit the documentation site for ArcSight.

Contact Information

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

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

1 Welcome to Fusion 1.5.1

Fusion provides the common elements needed for adding your users, accessing the Reports Portal, and using other core services that support portions of the ArcSight Platform in SaaS and non-SaaS environments:

- Create and use ArcSight dashboards to analyze data
- Access the Reports Portal to create visuals and reports for analyzing data
- Hunt for threats and vulnerabilities with built-in reports
- Access ArcMC to manage and monitor components in the ArcSight infrastructure
- Manage your MSSP profile and submit monthly EPS usage reports
- Manage users and groups
- Manage your user profile

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 ArcSight Recon
- Responding to and mitigating cyber attacks with ArcSight SOAR

To help you get started, Fusion 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.

- Chapter 2, "Viewing a Dashboard," on page 15
- Chapter 3, "Viewing Analyst and Entity Details," on page 17
- Chapter 4, "Managing Dashboards and Content," on page 19
- Chapter 5, "Configuring Widgets," on page 27

2 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.

- "View Data in a Dashboard" on page 15
- "View a Different Dashboard" on page 15

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

View Data in a 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" on page 15
- "All Available Dashboards" on page 15

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.

3 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" on page 17
- "Review Entities" on page 17

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

Select an entity in a widget.

If your environment incorporates data from ArcSight Intelligence, 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 Intelligence UI, where you can view the details of the risky entities of the selected entity type.

  NOTE: You can also navigate to the Entities page in the Intelligence UI in the following ways:

  - When you have deployed only Intelligence, click ENTITIES AT RISK in the left pane.
  - When you have deployed 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 Intelligence UI, where you can explore the risky activities associated with the entity.

4 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.

- "Change the Time Range of Data in a Dashboard" on page 19
- "Mark a Dashboard as a Favorite" on page 19
- "Specify a Default Dashboard" on page 20
- "Create or Clone a Dashboard" on page 20
- "Edit the Dashboard" on page 21
- "Import and Export a Dashboard" on page 22
- "Display a Dashboard on the SOC Screen" on page 23
- "Share a Dashboard" on page 23
- "Understand the Provided Dashboards" on page 24

Change the Time Range of Data in 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.

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.

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" on page 20
- "Clone a Dashboard" on page 21

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.

Edit the Dashboard

While viewing a dashboard, select ✎.

You can only modify the configuration of the dashboard that you are currently viewing, such as changing widget properties or adding and removing widgets.

- “Add Widgets” on page 21
- “Modify a Widget’s Properties” on page 21
- “Rearrange the Order of Widgets” on page 22
- “Remove Widgets” on page 22
- “Change the Dashboard’s Name” on page 22

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.

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" on page 23
- "Import a Dashboard" on page 23
- "Export a Dashboard" on page 23

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.

  NOTE: 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.

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.

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.

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

Understand the Provided Dashboards

These dashboards are not available in a SaaS environment.

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.

- "How is My SOC Running?" on page 24
- "Entity Priority" on page 25
- "Entity Risk" on page 25
- "Health and Performance Monitoring" on page 26

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. Alternatively, administrators can create one or more clones based on these dashboards, then share the clones, and set default dashboards for roles.

How is My SOC Running?

You must have the ESM Command Center capability deployed. This dashboard is not available in a SaaS environment.

The out-of-the-box 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

You must have the Layered Analytics capability deployed. This dashboard is not available in a SaaS environment.

The out-of-the-box dashboard, **Entity Priority**, combines content from both ArcSight Intelligence and ESM to provide the status of users and entities at risk, including risk scores calculated by Intelligence. It includes the following widgets:

- Active Lists
- Entity Count Overview

Entity Risk

You must have the Intelligence capability deployed.

The out-of-the-box 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 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 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 Intelligence User's Guide.

NOTE: You cannot modify the **Entity Risk** dashboard. You can only clone it.

Health and Performance Monitoring

This dashboard is not available in a SaaS environment.

The out-of-the-box dashboard, **Health and Performance Monitoring**, provides information about the status of the database used by capabilities such as ArcSight Recon and Intelligence. It includes the following widgets:

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

5 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" on page 27
- "Understand the Provided Widgets" on page 29

Understand Widget Properties

When you configure a widget, you might see a combination 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**, 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.

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.

NOTE: 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.

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” on page 29
- “Analytics Pipeline” on page 29
- “Case Breakdown” on page 30
- “Case Load” on page 30
- “Case Timeline” on page 31
- “Case Workflow Analysis” on page 31
- “Database Event Ingestion Timeline” on page 31
- “Database Cluster Node Status” on page 31
- “Database Storage Utilization” on page 32
- “Entity Count Overview” on page 32
- “Overall Risk Level” on page 32
- “Productivity” on page 33
- “Threat Analysis Funnel” on page 33
- “Top Risky Entities” on page 34

Active List

Requires data collection from ArcSight Intelligence and ArcSight ESM for best effect.

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

Analytics Pipeline

Requires data collection from ArcSight Intelligence.

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**.

NOTE: You can select the orientation for the **Analytics Pipeline** widget only if you use it in a clone of the **Entity Risk** out-of-the-box dashboard, a new dashboard, or an existing dashboard that is not out-of-the-box. You do not have the provision to select the orientation for the **Entity Risk** out-of-the-box dashboard.

Case Breakdown

Requires data collection from ArcSight ESM.

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 data collection from ArcSight ESM.

To help managers balance the amount of work assigned to case owner, 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, we recommend 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 data collection from ArcSight ESM.

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 data collection from ArcSight ESM.

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.

NOTE: 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 Event Ingestion Timeline

Requires that at least one deployed capability includes a 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 Cluster Node Status

Requires that at least one deployed capability includes a 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 Storage Utilization

Requires that at least one deployed capability includes a 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.

Vertica Eon mode supports use of a third party storage location technology, shared among it’s database nodes on premises or cloud. This shared storage location is also called Communal Storage and represented in the associated widget.

NOTE: The computational and communal layers of the Eon mode 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: Eon Mode Concepts.

Entity Count Overview

Requires data collection from ArcSight Intelligence.

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 Intelligence UI, where additional information for the selected entity type is displayed.

Overall Risk Level

Requires data collection from ArcSight Intelligence.

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 data collection from ArcSight ESM.

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.

Threat Analysis Funnel

Requires data collection from ArcSight ESM.

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 **percent** 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, it is possible for an increase to occur in 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 data collection from ArcSight Intelligence.

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 Intelligence UI, with the selected entity's name applied to the **anomalies and violations** filter.

NOTE: Note: You can change the filter for the **Top Risky Entities** widget only if you use it in a clone of the **Entity Risk** out-of-the-box dashboard, a new dashboard, or an existing dashboard that is not out-of-the-box. You do not have the provision to change the filter for the **Entity Risk** out-of-the-box dashboard.

II 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.

6 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" on page 37
- "View a Report" on page 37
- "Specify Default Dashboards for the Reports Portal" on page 38

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 you want to view.

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

2 Expand the desired category, then select the report that you want to view.

3 To change the time range, complete the following steps:

3a To activate the Calendar, point your cursor at the position of the **Calendar** icon to the right of the time selection box.

3b Select the **Calendar** icon.

3c Enter the **Start Time** for the report.

3d Enter the **End Time** for the report.

4 Select **Submit**.

The report will execute and display when it is complete.

5 (Optional) To email the report when it completes, select **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 Attacks and Suspicious Activity, and Denial of Service Activity dashboards.

To specify default dashboards:

1 Select **Reports** > **Portal** > **Portal Dashboards**.

2 Specify a name for your default dashboard.

3 (Optional) Enter a description for your dashboard portal.

4 Select one of the available dashboards.

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

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

6 Click **OK**.

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

7 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.

8 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.

9 Adding and Removing Report Content

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

Select **REPORTS** > **Content**.

The Reports **Content** enables administrators to modify the reports and dashboards in the following ways:

- Add and remove content, also known as assets, for the reports and dashboards using the **Import Assets** and **Export Assets** feature.
- Connect to data sources using the **Add Data Source** feature. Using this feature, you can gather content from specific sources to supply reports and dashboards.

Import and Export Content

This capability is not available in a SaaS environment.

Use the **Import Assets** and **Export Assets** options to manage the reports and dashboard available to your users. You can move assets from one server environment to another. For example, you might want to move a set of reports from a test server to a production server.

NOTE: If Reporting generates errors when you attempt to export assets, you should reduce the number of assets that you export concurrently.

Alternatively, you might need to increase the RAM for the Reporting node. For more information about sizing your environment for the workload, see the *Technical Requirements for ArcSight Platform*. However, in a SaaS environment you will not be able to adjust the RAM for the Reporting node.

Supported Data Sources

This capability is not available in a 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.

NOTE: The process for adding this type of data source is the same as for adding an Elasticsearch data source.

R

Connects to an R database containing R language sources.

10 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" on page 45
- "Using Data Models to Build a Worksheet" on page 47
- "Use Data Worksheets to Build a Dashboard or Report" on page 47
- "Create a Simple Dashboard" on page 48
- "Create a Simple Scheduled Report" on page 49
- "Creating a Simple Report" on page 50

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" on page 45
- "Build a Dashboard Using Search Results" on page 46
- "Convert the Search Fields to Human-Readable Values" on page 46

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.

Using Data Models to Build a Worksheet

Select **Reports** > **Reports Designer** > ***Report type*** > **Data Source** > **Database**.

Data models are logical models of the events table in the database that allow for an extra level of abstraction where you can perform varied transformations. You can use the final data model as the final table when creating a data worksheet. By default, the system has two data models:

Basic Data Model

Contains fewer columns from the events table. Use this model for an easier understanding or for simple reports that require less fields.

Event View

Contains the entire events table.

You can also create, edit, and delete your own Data Models. For more information, see “Create a Data Model” in the Help in the Reports Portal. Make sure to add only the fields you that need and create the filters from there. Some of the fields in the data model are non-human readable. You should parse them to ensure that they are readable in the report.

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.

6 (Conditional) To refine the design, select one of the following options from the **Preview** pane.

For example, you can sort and reorder the columns or change the data mode.

7 To save your changes, complete the following steps:

  7a Select **Save** or **Save As**.

  7b Specify the folder where you want to save the worksheet.

  Do not specify the **Standard Content** folder, which is reserved for the built-in reports and dashboards.

8 Exit the Data Worksheet as needed.

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" on page 48
- "Use the Dashboard Editor" on page 49

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 Simple Scheduled Report

You can create a report that runs on your chosen schedule. In the report, define conditions that trigger tasks and actions you want to run.

1. Select **Reports** > **Scheduler**.
2. In the lower left corner of the screen, select **New Task**.
3. For **Name**, enter a name of the task.
4. To set the conditions for your report, complete the following steps:

   4a Select the **Condition** tab.

   4b (Conditional) To specify the timezone that the report uses, perform one of the following actions:

   - To use the timezone where the server is installed, select **Show Server Time Zone**.
   - To use your timezone, deselect **Show Server Time Zone**.

   4c (Conditional) To run the task at specific intervals, configure the frequency.

   For example, to run a report every Monday afternoon, specify the following settings:

   - Select **Time Range**, then **Afternoon**.
   - For **Every**, enter 1
   - Select **Monday**.

   4d (Conditional) To run the tasks in sequence, select **Chained**, then specify the first task.

   4e Select **OK** to save the scheduled task.
5. To specify the report associated with the scheduled tasks, complete the following steps:

   5a Select the **Action** tab.

   5b For **Report**, click **Select** then navigate to the report that you want to schedule.

   5c To email the report results, select **Deliver to Emails** then configure the email content and destination addresses.

5d To set the time range in which the report retrieves data, complete one of the following actions:

- Select **Add**, and then specify the time values.
- Select **Creation Parameters**, then choose the dates from the calendar option.

5e Select **OK** to save your changes.

Creating a Simple Report

First, create and save a data worksheet. For additional details on how to create a data worksheet, see Using Data Worksheets to Build a Dashboard or Report.

Use the one of the following wizards to create a simple report.

- "Use the Crosstab Wizard" on page 50
- "Use the Table Wizard" on page 50
- "Use the Chart Wizard" on page 51
- "Guidelines for Report Usage" on page 51

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 bundled dashboards from the Recon Installation and use them as templates for other creations.

III Hunting for Threats and Vulnerabilities

Available only with ArcSight capabilities.

To help you hunt for undetected 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 report and dashboards focus on fundamental security issues, such as monitoring firewalls and malware. For rapid access to your regular dashboards, you can configure the Reports Portal to display those dashboards by default.

- Chapter 11, “Understanding the Cloud Security Dashboards and Reports,” on page 55
- Chapter 12, “Understanding the Foundation Dashboards and Reports,” on page 65
- Chapter 13, “Understanding the OWASP Security Dashboards and Reports,” on page 73

11 Understanding the Cloud Security Dashboards and Reports

Available only with ArcSight capabilities.

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

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

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

Category	Dashboards	Reports
Abuse and Nefarious Use of Cloud Services	DoS Originated from EC2 Instances 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	*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*

Category	Dashboards	Reports
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
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, usually forwarded from ArcSight Enterprise Security Manager. 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 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	*n/a*

DoS Originated from EC2 Instances

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

EC2 Instances Communicating with Cryptocurrency Entity

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

EC2 Instances Querying Domains Involved in Phishing Attacks

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

EC2 Machines Involved in Suspicious Communication

Lists the EC2 machines that are involved in suspicious communication.

Email Spam Originated from EC2 Instances

Identifies email spam that originates from EC2 instances.

Nefarious Activity by an Unauthorized Individual from EC2

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

Suspicious Activity Reported by Microsoft Azure

Lists suspicious activity reported by Microsoft Azure.

Trojans or Backdoors Installed on EC2 Instances

Lists backdoors or trojans discovered on EC2 machines.

Account Hijacking

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 Attacks

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

Phishing Attacks

Provides charts that show the phishing attacks against the 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. This dashboard also is available within the Abuse and Nefarious Use of Cloud Services category.

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.

Dashboards	Reports
All Information Leakage Events Information Disclosure Vulnerabilities Organizational Information Leakage Personal Information Leakage	*n/a*

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

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.

Amazon AWS Deletion Events

Provides charts and a table listing the number of deletion events by operations, day, source address, and source user

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.

Dashboards	Reports
DoS Activity	*n/a*

DoS Activity

Provides charts the top source and destination addresses, as well as events by day. This dashboard also is available within 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 multi-customer 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.

12 Understanding the Foundation Dashboards and Reports

Available only with ArcSight capabilities.

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

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

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

Category	Dashboards	Reports
Vulnerability Monitoring	Vulnerability Overview	High Risk Vulnerabilities by Host SSL Vulnerabilities Vulnerability Summary 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.

Dashboards	Reports
Account Management Overview Failed Logins Overview Successful Login Overview	All Logins by Hostname Failed Logins Summary Login Activity by User

Account Management Overview

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

All Logins by Hostname

Reports the number of login attempts over time, including the outcome, for the specified hosts.

You must specify one IP address.

Failed Logins Overview

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

Failed Logins Summary

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

Login Activity by User

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

You must specify one user by `Destination UserName`.

Successful Login Overview

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

Events Overview

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.

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.

Dashboards	Reports
n/a	Anti-virus Activity Audit Log Cleared Events Failed Anti-virus Updates Summary Operating System Errors and Warnings Services Shutdown Services Started

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.

Dashboards	Reports
Malware Overview	Reported Malware by Host Worm Infected Systems

Malware Overview

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

Reported Malware by Host

Lists the malware found on the specified hosts.

You must specify one host.

Worm Infected Systems

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

Network Monitoring

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

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

Dashboards	Reports
Attacks and Suspicious Activity Overview DGA Overview DoS Activity Email Attacks IDS Events Man in the Middle Atacks Reconnaissance Activity Traffic Anomaly Overview VPN Activities Overview	Exploit Attempts Detected by IDS Network Device Configuration Changes

Attacks and Suspicious Activity Overview

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

This dashboard also is available in the Insufficient Logging and Monitoring category of the **OWASP** reports.

DGA Overview

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

DoS Activity

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

This dashboard also is available in the Denial of Service category of the **Cloud** reports.

Email Attacks

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

Exploit Attempts Detected by IDS

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

IDS Events

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

Man in the Middle Atacks

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

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

Network Device Configuration Changes

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

Reconnaissance Activity

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

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

Traffic Anomaly Overview

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

VPN Activities Overview

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

Perimeter Monitoring

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.

Dashboards	Reports
Firewall Blocked Events Firewall Traffic Overview	Firewall Configuration Changes Firewall Blocked Traffic by Destination Address

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.

Dashboards	Reports
Vulnerability Overview	High Risk Vulnerabilities by Host SSL Vulnerabilities Vulnerabilities by Host XSRF Vulnerabilities XSS Vulnerabilities

High Risk Vulnerabilities by Host

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

You must specify one host by `Destination Host`.

SSL Vulnerabilities

Lists the hosts reported to have the most SSL vulnerabilities.

This report also is available in the Using Components with Known Vulnerabilities category of the **OWASP** reports.

Vulnerability Overview

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

Vulnerabilities by Host

Lists all vulnerabilities found on the specified hosts.

You must specify one IP address.

XSRF Vulnerabilities

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

XSS Vulnerabilities

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

13 Understanding the OWASP Security Dashboards and Reports

Available only with ArcSight capabilities.

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

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

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

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

Category	Dashboards	Reports
Using Components with Known Vulnerabilities	SSH Vulnerabilities Overview Vulnerability Overview	SSH Vulnerabilities Summary SSL Vulnerabilities
XML External Entities	XML Vulnerabilities Overview	XML Vulnerabilities

Broken Access Control

Select Reports > Portal > Repository > Standard Content > OWASP > A 5 - Broken Access Control.

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

Dashboards	Reports
n/a	Broken Access Control

Broken Access Control

Lists vulnerable hosts by severity over time.

Broken Authentication

Select Reports > Portal > Repository > Standard Content > OWASP > A 2 - Broken Authentication.

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.

Cross-site Scripting

Select > Reports > Portal > Repository > Standard Content > OWASP > A 7 - Cross-Site Scripting.

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

Dashboards	Reports
Cross Site Scripting	XSS Vulnerabilities

Cross Site Scripting

Lists events associated with XSS vulnerabilities.

XSS Vulnerabilities

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

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

Injections

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 1 - Injections**.

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

Dashboards	Reports
Injection Vulnerabilities Overview	Command Injections on HTTP Request 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.

Injection Vulnerabilities

Lists the hosts with the most injection vulnerabilities over time.

Injection Vulnerabilities Overview

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

SQL Injection

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

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

Insecure Deserialization

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 8 - Insecure Deserialization**.

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

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.

Insufficient Logging and Monitoring

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 10 - Insufficient Logging and Monitoring**.

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

Dashboards	Reports
Attacks and Suspicious Activity Failed Logins Overview Login Activity Overview Operating System Errors and Warnings Security Log is Full	All Logins by Hostname Audit Log Cleared Failed Logins Summary

All Logins by Hostname

Lists all logins that have occurred on the specified host.

Attacks and Suspicious Activities Overview

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

This dashboard also is available in the Network Monitoring category of the **Foundation** reports.

Audit Log Cleared

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

Failed Logins Overview

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

Failed Logins Summary

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

Login Activity Overview

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

Operating System Errors and Warnings

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

Security Log is Full

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

Security Misconfiguration

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 6 - Security Misconfiguration**.

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

Dashboards	Reports
Misconfiguration Events Overview Missing Security Patches Overview	Security Patch Missing

Misconfiguration Events Overview

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

Missing Security Patches Overview

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

Security Patch Missing

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

Sensitive Data Exposure

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 3 - Sensitive Data Exposure**.

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

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.

Using Components with Known Vulnerabilities

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 9 - Using Components with Known Vulnerabilities**.

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

Dashboards	Reports
SSH Vulnerabilities Overview Vulnerability Overview	SSH Vulnerabilities Summary 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.

XML External Entities

Select **Reports** > **Portal** > **Repository** > **Standard Content** > **OWASP** > **A 4 - XML External Entities**.

Older or mis-configured XML processors use XML documents to evaluate external entity references, and can inadvertently process harmful XML input. Malicious users 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.

Dashboards	Reports
XML Vulnerabilities Overview	XML Vulnerabilities

XML Vulnerabilities

Lists the hosts with the most XML vulnerabilities.

XML Vulnerabilities Overview

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

IV Accessing ArcMC

Available only with ArcSight capabilities. Not available in a 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.

- Chapter 14, "Accessing Bulk Operations," on page 83
- Chapter 15, "Accessing ArcMC Dashboards," on page 85

14 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

15 Accessing ArcMC Dashboards

Select **ARCMC** > **Dashboards**.

The dashboards enable you to view the health and status of the components that ArcMC manages.

V Managing Your Service Provider Contracts

To use this feature, you must have an MSSP contract with Micro Focus.

Select **ADMIN** > **Contract & Usage**.

Micro Focus 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.

Fusion 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 Guide to Reporting EPS Usage*.

16 Managing Your MSSP Contracts

Select **ADMIN** > **Contract & Usage** > **Contracts**.

Micro Focus 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 a Micro Focus MSSP contract to pay-per-use, with an entitlement of one or more of Transformation Hub, Intelligence or Recon but without the initial cost of deploying the ArcSight Platform and Fusion in your IT environment. Each contract has a set length of time before it expires. You can access and use Fusion as long as you have a valid contract.

The MSSP contracts charge you basis EPS (events per second) usage. Micro Focus 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, Micro Focus charges you more for the service. You can see the tiers and the rates for each tier in ArcSight Platform and Fusion. 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 Micro Focus, you receive a copy of that contract. You must add the contract received to ArcSight Platform and Fusion you purchased. The contract also includes a signature file that Micro Focus uses to verify whether the contract you added is valid or not.

When you add the contract to ArcSight Platform and Fusion, Micro Focus 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.

NOTE: If your contract expires or is going to, request Micro Focus for a new contract file.

17 Reviewing and Reporting EPS Usage

Select **ADMIN** > **Contract & Usage** > **Monthly Usage Details**.

Fusion allows you to view your events per second (EPS) usage and the rates that Micro Focus charges in a single location. Fusion provides daily averages of your usage and an aggregate of your month-over-month usage and rates.

IMPORTANT: It is possible that the bill you receive from Micro Focus might not match the cost displayed in the monthly report that you send to Micro Focus. The monthly report provides usage information, but Micro Focus could adjust the total cost, which results in a different invoiced amount. If you have any questions, please contact your Micro Focus representative.

- "Review Monthly Usage" on page 91
- "Submit an EPS Usage Report" on page 92

Review Monthly Usage

Select **ADMIN** > **Contract & Usage** > **Monthly Usage Details**.

Fusion 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.

NOTE: 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, Fusion 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**.

Fusion 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 Micro Focus and the email distribution list.
- Set up a monthly reminder for sending the reports.

NOTE: To email PDF or CSV files from Fusion, 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 Fusion will not be able to send the emails.

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.

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.

18 Managing Your MSSP Profile

Select **ADMIN** > **Contract & Usage** > **Profile**.

The MSSP Profile shows your account number and name from the contract, along with your contact information, while Fusion distributes the usage reports. You cannot access any of the sections of the MSSP Profile unless you add your contract to ArcSight Platform and Fusion. Also, to support emailing reports, your ArcSight Platform admin must set up an SMTP server.

- "Edit the MSSP Profile" on page 93
- "Configure Distribution of the Usage Reports" on page 94

Edit the MSSP Profile

Select **ADMIN** > **Contract & Usage** > **Profile**.

To be able to distribute the Fusion 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 partiality configured MSSP profile to have Fusion 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 and Fusion.
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 Fusion 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 Fusion does not send the emails, then.

- "Send Reports Automatically" on page 94
- "Set Up a Monthly Reminder" on page 94
- "Create an Email Distribution List" on page 94

Send Reports Automatically

Fusion can automatically send the usage reports to Micro Focus and your email list. Fusion 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 Micro Focus 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

Fusion 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.

VI 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*.

19 Assigning Permissions to Roles

You must have the appropriate permissions to create roles and assign permissions.

Click **ADMIN** > **Roles and Permissions**.

Fusion 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.

- "Available Permissions" on page 97
- "Default Roles" on page 101
- "Create a Role with Permissions" on page 102
- "View Details of a Role" on page 103

Available Permissions

Some permissions are available for any deployed product. Other permissions depend on the capabilities that you have deployed.

- "Reports Permissions" on page 97
- "User Management Permissions" on page 98
- "ArcSight Permissions" on page 99

Reports Permissions

The following table lists the permissions available when you add the Reports feature.

Function	Permission	Allows users to...
Reports	Report Admin	In the Reports Portal ... - View dashboards and reports - Create subfolders - Schedule reports - Create data worksheets, dashboards, and reports - View Admin reports - Manage the data source *(not available in a SaaS environment)*

Function	Permission	Allows users to...
Reports	Design Reports	In the Reports Portal ... - View dashboards and reports - Create subfolders - Schedule reports - Create data worksheets, dashboards, and reports
Reports	Schedule Reports	In the Reports Portal ... - View dashboards and reports - Create subfolders - Schedule reports
Reports	View Reports	In the Reports Portal ... - View dashboards and reports - Create subfolders

User Management Permissions

The following table lists the permissions needed to manage users.

Function	Permission	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
User Management	Assign Roles to Users	- View users - Assign roles that you currently have to users that you manage

Function	Permission	Allows users to...
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 roles 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 Recon or Intelligence.

Function	Permission	Allows users to...	Available with...
ArcMC	ArcMC System Admin	- Perform System Admin functions *(not available in a SaaS environment)*	ArcMC
ArcMC	ArcMC Operation Admin	- Perform all Operations functions, but does not have access to System Admin *(not available in a SaaS environment)*	ArcMC
ArcMC	ArcMC System Viewer	- Read only access to System Admin functions *(not available in a SaaS environment)*	ArcMC
ArcMC	ArcMC Operation Viewer	- Read only access to Operations functions *(not available in a SaaS environment)*	ArcMC

Function	Permission	Allows users to...	Available with...
Dashboards	Share a Dashboard	- With the **Manage Role** permission, share the current dashboard with any role - Without the **Manage Role** permission, share the current dashboard with any of the roles associated with the user's role	Fusion
Intelligence	Access Intelligence	- Log in and use Intelligence	Intelligence
Intelligence	View Intelligence Raw Events	- Access Intelligence - View raw event data	Intelligence
Intelligence	Tune Intelligence Analytics	- Access Intelligence - Fine-tune the importance applied by Analytics to the events in your source data	Intelligence
Intelligence	Access Intelligence Search Manager	- Access Intelligence - Use the Intelligence Search Manager tool for troubleshooting **NOTE:** Do not assign this permission or use the tool without first consulting Support Services. For more information, see the *ArcSight Intelligence User Guide* on the ArcSight Intelligence documentation site. In a SaaS environment, this permission is available only to the System Operations Administrator.	Intelligence
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
Searches	Execute Search	- Execute searches using fieldsets, custom ranges dates, and search operators	Recon *Also available for ESM, Intelligence, and SOAR in a preview mode*
Searches	Export Search Results	- Export the search results in csv format	Recon *Also available for ESM, Intelligence, and SOAR in a preview mode*
Searches	Never Expire Search Results	- Configure searches to never expire	Recon
Searches	Manage Scheduled Searches	- Create and manage scheduled searches	Recon

Function	Permission	Allows users to…	Available with…
Searches	Perform Event Integrity Check	- Run an Event Integrity Check and view the results	Recon
Searches	Manage Outlier Models and Scoring	- Create and delete Outliers models - Build and pause the scoring processes	Recon
Searches	Manage Lookup Lists	- Add, configure, view, and delete lookup lists	Recon
Searches	Manage Fieldsets	- Create, edit, and delete fieldsets	Recon
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	Recon *Also available for ESM, Intelligence, and SOAR in a preview mode*
Searches	Logger Data Migration	- Execute a data migration to Recon from Logger	Recon
Operations Management	Access Database Monitoring	- Access the APIs for monitoring the database *(not available in a SaaS environment)*	Capabilities that require the ArcSight Database
Operations Management	Manage Storage Groups	- Create and manage storage groups	Recon
Operations Management	Manage Kafka	- Access Kafka Manager for Transformation Hub *(not available in a SaaS environment)*	Transformation Hub

Default Roles

Fusion 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 only when their associated capability, such as Reports or ArcSight Recon, is deployed.

NOTE: As of the Fusion 1.4 release, some roles are no longer default roles. However, Fusion 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	- All permissions

Default Role	Permissions
Admin	- All **Dashboard** permissions - All **Intelligence** permissions, except *Access Intelligence Search Manager* - All **Licensing and Usage** permissions - All **Reports** permissions - All **Searches** permissions - All **User Management** permissions - *Manage Storage Groups*
Analyst	- All **Dashboard** permissions - *Execute Search* - *Manage Fieldsets* - *Manage Search Queries/Criteria* - *Access Intelligence* - *View Intelligence Raw Events* - *Schedule Reports* - *View Reports*
System Operations Administrator *Not available to customers in a SaaS environment*	- All **Dashboard** permissions - All **ArcMC** permissions - *Access Intelligence Search Manager* - *Access Database Monitoring* - *Manage Kafka*

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 permssions 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:

  5a Select the **USERS** tab.

  5b Select **Assign role to users**.

  5c Choose the users you want to add to the role.

  5d **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 permssions and roles that you have yourself.
   - Add or remove users
   - Delete the role

Change Permissions for the Role

You can only assign permssions 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.

20 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.

Import Users from ArcSight Enterprise Security Manager

This function is not available in a SaaS environment.

To help you get started, you can import users already authorized for ESM. You need to have at least one role available in Fusion to assign to these users.

Click **ADMIN** > **Users and Groups** > *group_name*.

For more information, see the *Administrator Guide for ArcSight Platform*.

View Details of a Group

When you view the details of a user group, you can also modify the group's membership.

1. Click **ADMIN** > **Users and Groups** > *group_name*.
2. You can also perform the following actions:
   - Add or remove users from this or other groups
   - Add or remove managers from the current group
   - Assign or remove roles for users in the current 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.

In a SaaS environment, administrators and managers cannot create or change the password in a user's profile. Only users can specify and reset their passwords.

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, to specify or change the user's password, complete the following steps:

 6a Select **Users and Groups** > **Search Users**.

 6b Select the user that you just created.

 6c Click **RESET PASSWORD**.

 6d Enter the password, then click **SAVE**.

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 assigments

Change the User’s Password

This function is not available in a 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.

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.

VII 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 and interface theme.

21 Manage Your Account

Select *[your_ID]* > **My Profile** > **MY PROFILE**.

You can change your account settings. However, you cannot change your password in Fusion if your enterprise uses an external authentication method.

22 Configure Your User Preferences

Select ***[your_ID]*** > **My Profile** > **PREFERENCES**.

Some deployed capabilities enable you to configure preferences for commonly used settings. For example, in ArcSight Recon, if you regularly use the same fieldset for a Search, you can specify that set as your preferred default.

- "Configure Search Preferences" on page 113

Configure Search Preferences

Available only when ArcSight Recon is deployed in your environment.

To reduce the time required to create and manage searches, configure Search to use your preferred settings. You can always override your preferences as needed when you create a search.

Default Fieldset

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

Default View

Specifies whether you want the Events Table to display results in the **Grid View** or **Raw View**. The default value is *Grid View*.

Time Zone

Instructs Search to adjust the timestamp for events to the chosen time zone.

- Browser
- Database
- Custom

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

Date / Time Format

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

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

Default Time Setting

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

- **Dynamic**

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

- **Static**

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

- **Preset**

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

Base Searches On

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

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

Search Expires In

Specifies how often you want searches to expire, and thus be removed from the system. You can also choose to never remove a search.

Maximum Search Results

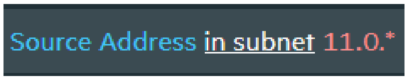
Specifies the maximum number events that the Search will return. You can specify a value between 1 and 10 million. The default is *300,000*.

Highlight Query Syntax

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

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

Figure 22-1 *Example of Highlighted Query Syntax*



Source Address in subnet 11.0.*

23 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.

24 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.