Hewlett Packard
Enterprise

# HPE Security ArcSight ESM: Reconnaissance

Software Version: 1.0

Security Use Case Guide

April 3, 2017

# Legal Notices

## Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

## Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice



Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

# Support

## Contact Information

| | |
|---|---|
| **Phone** | A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list |
| **Support Web Site** | https://softwaresupport.hpe.com |
| **Protect 724 Community** | https://www.protect724.hpe.com |

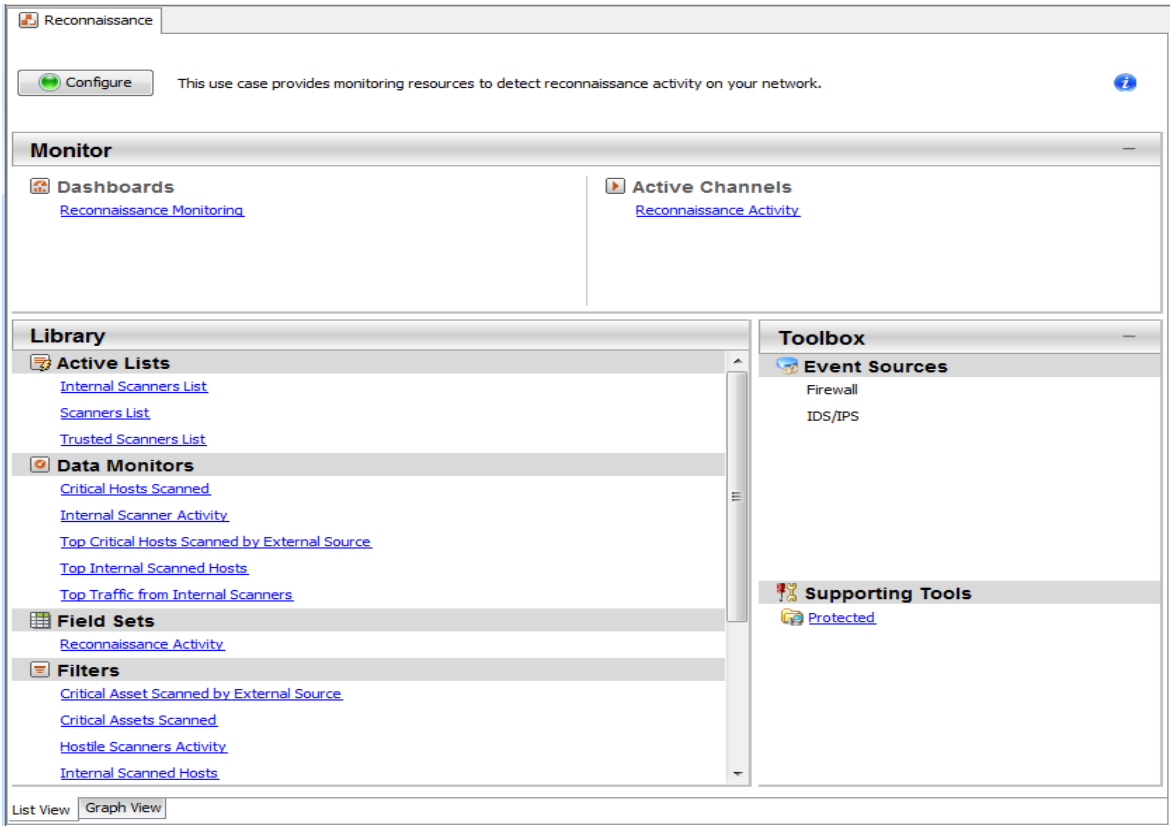
# Contents

# Chapter 1: Overview

Reconnaissance is an information-gathering activity that scans for vulnerabilities in your network. Scans can come from external or internal source; and they target either hosts, or ports on a host. An abundance of this activity can indicate an eminent attack, when a vulnerability is found.

The Reconnaissance Security Use Case monitors such activities and displays them on data monitors and an active channel, which you access from the dashboard. The information collected by the use case helps you investigate, then take actions on scanners and the scanned critical hosts.

The Reconnaissance use case contains the following resources:




- A **dashboard** (Reconnaissance Monitoring) is your starting point to monitor reconnaissance activities. The dashboard provides access to the data monitors that show information on targeted critical hosts, internal scanners, and top traffic activity.
- An **active channel** (Reconnaissance Activity) shows all reconnaissance events within a given timeframe.
- A **rule** (Reconnaissance from Internal Source) looks for reconnaissance activity from internal sources. Information is written to two active lists. You can further configure this rule to send notifications and create cases.

Access the Reconnaissance use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard and the active channel used to monitor and investigate reconnaissance activity. The Library section of the use case lists all supporting resources that help collect information that goes on the dashboard and active channel.

The use case also provides a configuration wizard that guides you through required configuration.

This document describes how to install, configure, and use the Reconnaisance use case and is designed for security professionals who have a basic understanding of ArcSight ESM and are familiar with the ArcSight Console. For detailed information about using ArcSight ESM, see the ArcSight ESM help system from the ArcSight Console **Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

**Note:** With regard to reconnaissance activities, the source is the scanner address and the destination is the scanned host.

# Chapter 2: Installation

To install the Reconnaissance use case, perform the following tasks in the prescribed sequence:

1. Download the Reconnaissance use case zip file from the ArcSight Marketplace into the ArcSight Console system where you plan to install the use case. Extract the zip file.
2. Log into the ArcSight Console as administrator.

   **Note:** During the package installation process, do not use the same administrator account to start another Console or Command Center session simultaneously. This login is locked until the package installation is completed.

3. Verify if you have a previous version of the use case package you want to install. If so, uninstall and delete this previous version:
   a. On the **Packages** tab of the Navigator panel, right-click the package and select **Uninstall Package**. The package icon is gray when it is uninstalled.
   b. Right-click the package and select **Delete Package**.
4. On the Packages tab, verify if **Downloads Groups** is already installed. If you see packages in `/All Packages/Downloads/Downloads Groups`, then ignore this step.

   If the Downloads Groups package is not present, import and install the *Downloads_Groups_1.0.arb* package. See "Importing and Installing a Package" on the next page for details.
5. Import and install the **Reconnaissance** use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the Reconnaissance resources. See "Assigning User Permissions" on page 8 for details.

# Importing and Installing a Package

This procedure assumes you have downloaded the zip file and extracted the contents into the ArcSight Console system. You must have administrator privileges to perform the tasks.

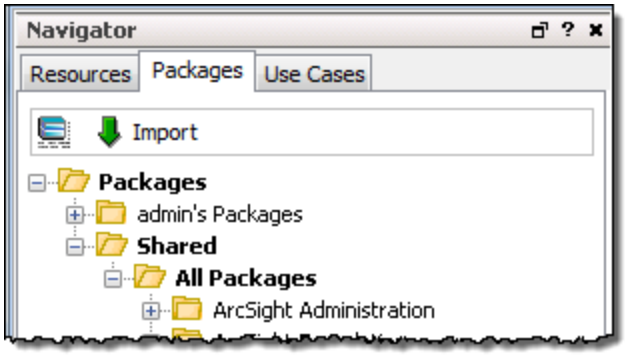
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install that package first. Then repeat the steps to import and install the **Reconnaissance** use case package.

  **Note:** The Downloads Groups package contains the groups used by the resources in the security use case; you must import and install this package first.

- If the Downloads Groups package is already installed, follow the steps to import and install the Reconnaissance use case package only.

### To import and install a package:

1. Log into the ArcSight Console as administrator. In the Navigator panel, click the **Packages** tab.




2. Click **Import**.
3. In the Open dialog, browse and select the `Reconnaissance_1.0.arb` package file you want to import, then click **Open**.

   The Importing Packages dialog shows how the package import is being verified for any resource conflicts.
4. In the Packages for Installation dialog, make sure that the check box is selected next to the name of the package you want to install and click **Next**.

   The Progress tab shows how the installation is progressing. When the installation is complete, the Results tab displays the summary report.
5. In the Installing Packages dialog, click **OK**. In the Importing Packages dialog, click **OK**.
6. On the **Packages** tab of the Navigator panel, expand the package group in `/All Packages/Downloads/` to verify that the package group is populated and that installation is successful.

# Assigning User Permissions

By default, users in the `Administrators` and `Default User Groups/Analyzer Administrators` user groups can view and edit ESM resources. Users in the `Default User Groups` (and any custom user group under this group) can only view Reconnaissance resources. Depending on how you set up user access controls within your organization, you might need to adjust those controls to make sure the resources are accessible to the authorized users.

**Note:** By default, the `Default User Groups/Analyzer Administrators` user group does not have edit permissions for archived reports in the Downloads group.

The following procedure assumes that you have logged into the ArcSight Console as administrator, and that you have set up the required user groups with the authorized users.

### To assign user permissions:

1. In the Navigator panel, open the **Resources** tab.
2. For each of the resource types provided in the use case, navigate to `Downloads/Hostile Activity Detection`.
3. Right-click the **Reconnaissance** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
4. Select the user groups for which you want to grant permissions and click **OK**.

# Chapter 3: Configuration

Before configuring the use case, make sure that you have populated your ESM network model. A network model keeps track of the network nodes participating in the event traffic. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

The Reconnaissance use case requires the following configurations for your environment:

- **SmartConnectors:** Install the appropriate ArcSight SmartConnectors to receive relevant events from your antivirus server. Examples are SmartConnectors for McAfee ePolicy Orchestrator DB and for Symantec AntiVirus Corporate Edition File.
  - Refer to the applicable SmartConnector guide for installation instructions.
  - Refer to the *ArcSight Console User's Guide* for instructions to register SmartConnectors in ESM.
- **Asset categorization:** Manually categorize all internal assets (assets inside the company network), or the zones to which the assets belong, with the **Protected** asset category. This category is located in `/All Asset Categories/Site Asset Categories/Address Spaces/Protected`). Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as Web servers) as Protected.

  In addition, configure which protected assets belong to either `/All Asset Categories/System Asset Categories/Criticality/`**`Very High`** or `/All Asset Categories/System Asset Categories/Criticality/`**`High`**.

  Refer to the topic, "Managing Asset Categories," in the *ArcSight Console User's Guide*.

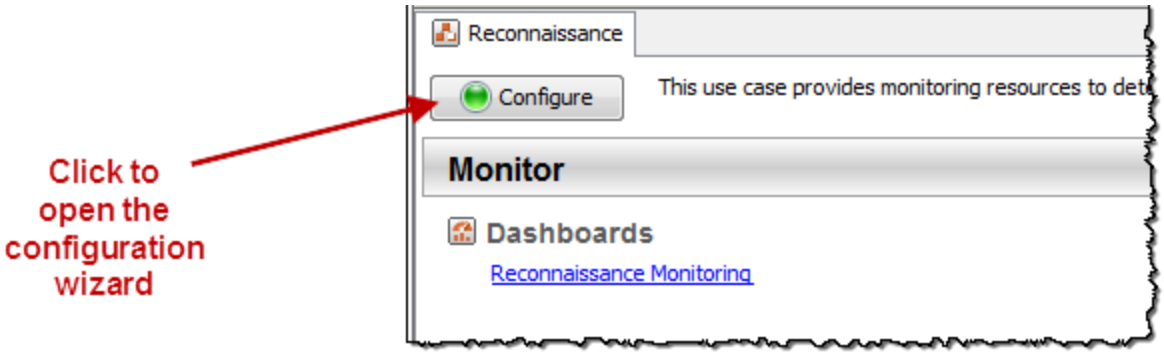
**Note:** You must categorize assets internal to the network manually; the procedure is not part of the use case configuration wizard.

### To configure the Reconnaissance use case:

1. In the Navigator panel, click the **Use Cases** tab.
2. Go to the **Reconnaissance** use case located in `/All Use Cases/Downloads/Hostile Activity Detection`.
3. Open the Reconnaissance use case: double-click the use case, or right-click the use case and select **Open Use Case**.

   The Reconnaissance use case lists all the resources used for monitoring reconnaissance activity.

4. Click the **Configure** button to open the configuration wizard.



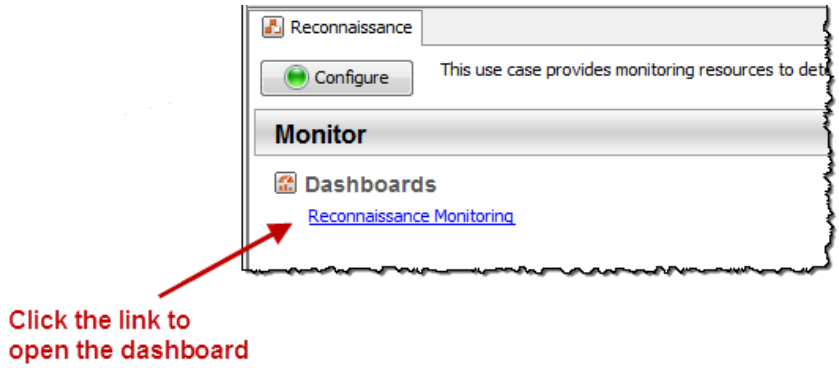

5. Click **Next** to follow the configuration steps.

After you configure the Reconnaissance use case, you are ready to monitor reconnaissance activity. See "Getting Started with the Reconnaissance Monitoring Dashboard" on page 11.

# Chapter 4: Getting Started with the Reconnaissance Monitoring Dashboard

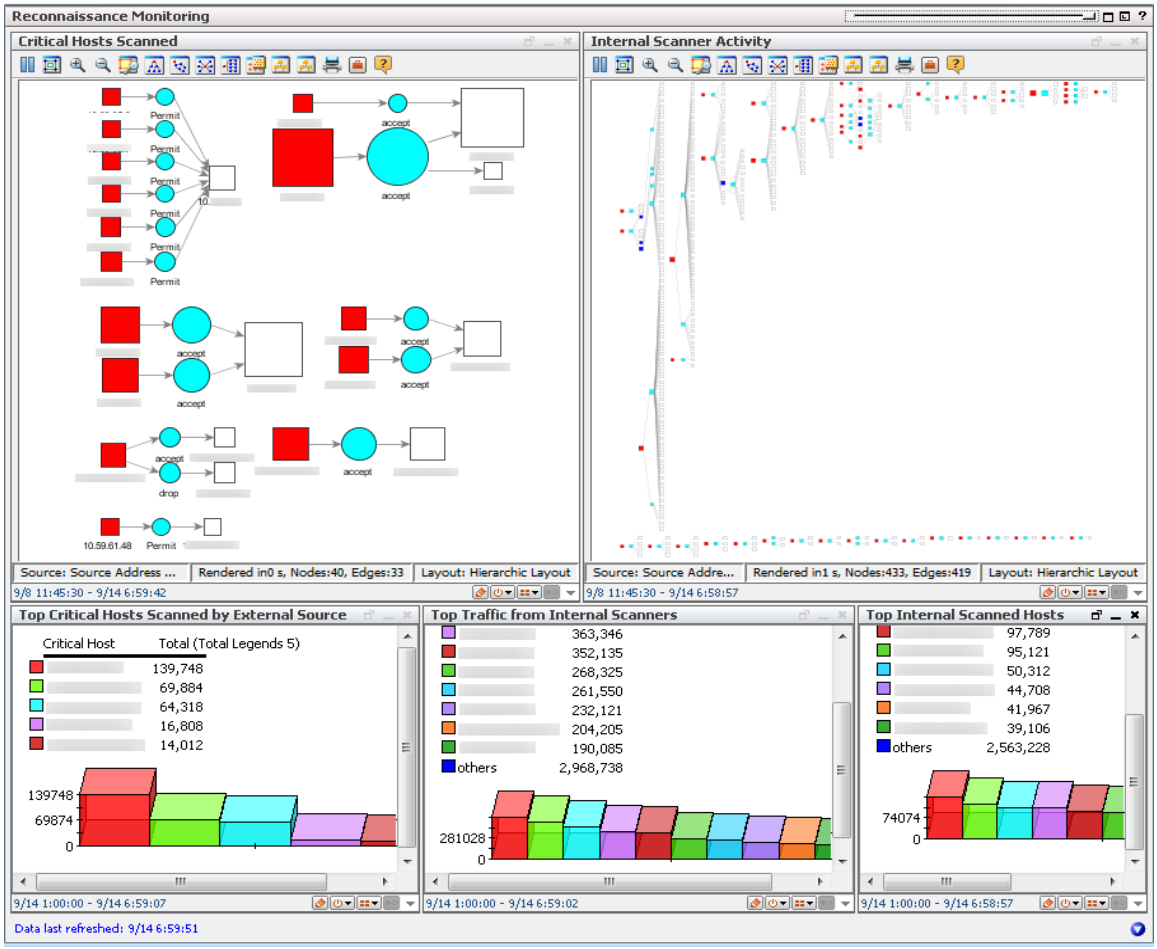
The Reconnaissance use case provides a dashboard to help you detect reconnaissance activities. Use this dashboard as a starting point for monitoring traffic scans into your network.

To open the dashboard, click the link for the dashboard in the Reconnaissance use case.




The dashboard opens in the Viewer panel of the ArcSight Console.

Following is an example of the dashboard:




The Reconnaissance Monitoring dashboard includes the following data monitors, from top left, clockwise:

- **Critical Hosts Scanned**

  Refer to "Using the Critical Hosts Scanned Data Monitor" on page 22 for details.
- **Internal Scanner Activity**

  Refer to "Using the Internal Scanner Activity Data Monitor" on page 15 for details.
- **Top Critical Hosts Scanned by External Sources**

  Refer to "Using the Top Critical Hosts Scanned by External Source Data Monitor" on page 25 for details.
- **Top Traffic from Internal Scanners**

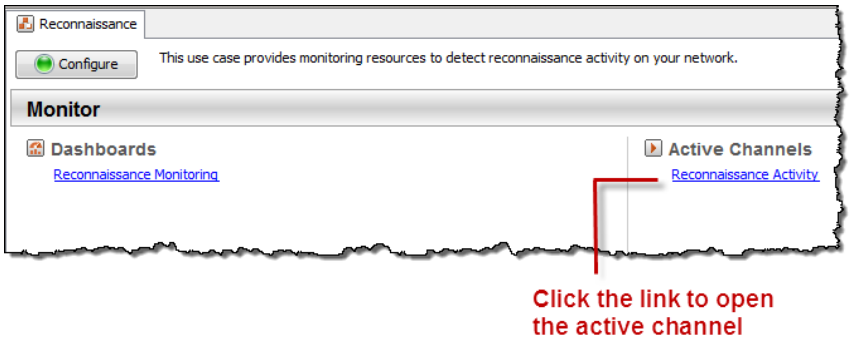
  Refer to "Using the Top Traffic from Internal Scanners Data Monitor" on page 18 for details.
- **Top Internal Scanned Hosts**

  Refer to "Using the Top Internal Scanned Hosts Data Monitor" on page 28 for details.

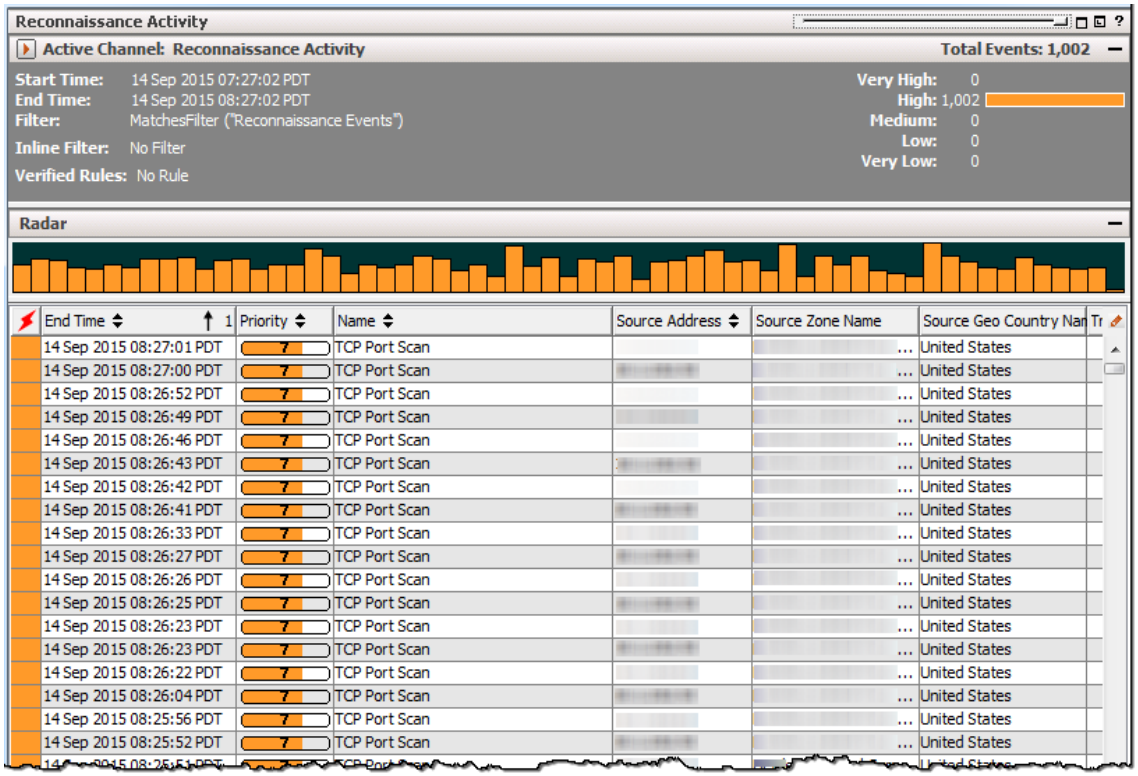
# Chapter 5: Monitoring the *Reconnaissance Activity* Active Channel

The active channel displays high-level information on all reconnaissance (attempts or successes) from all sources to all destinations.

To open the active channel, click the link on the Reconnaissance use case:




Following is an example of the Reconnaissance Activity active channel:



### To view the active channel:

- On the Reconnaissance use case's Active Channels section, click the **Reconnaissance Activity** link,

  Or
- On the Navigator > Resources panel:
  a. Go to `/All Active Channels/Downloads/Hostile Activity Detection/Reconnaisance.`
  b. Right-click **Reconnaissance Activity** and select **Show Active Channel**.

### To use the active channel:

- Right-click an item (such as an IP address) and select **Show Event Details** to see detailed information about the event. You can also create an inline filter to display events from a specific item.

  See the *ArcSight Console User's Guide*'s topic on using active channels for information about menu options and inline filters.
- Right-click on an event and select **Export**. Then select one of the available export options. Refer to the *ArcSight Console User's Guide*'s topic, "Exporting Events to a File," for more information.

**Note:** The events displayed in an active channel do not refresh automatically at ten-minute intervals. To refresh the view, click the **Stop** and **Replay** channel controls in the toolbar.

Depending on your environment, ESM load, and specific investigation needs, you can configure an active channel to use continuous, automatic channel refresh: Right-click the link for the active channel in the use case and select **Edit Active Channel**. From the Time Parameters drop-down on the Attributes tab of the Inspect/Edit panel, select **Continuously evaluate**.

**Note:** In a high EPS environment, you might see performance issues if you scroll down to try and view all the events in the active channel.

# Chapter 6: Monitoring Internal Scanners

This chapter provides information about reconnaissance scans coming from within your network. While you expect internal network activity to be routine, you need to differentiate between legitimate access and suspicious scans from sources that are not authorized to access certain hosts. The ArcSight resources for monitoring internal scanners help you identify internal scanners for further investigation. Suspicious scans from unauthorized internal sources might indicate that the internal scanner has been compromised and may be used for real attacks.

The following topics are covered:

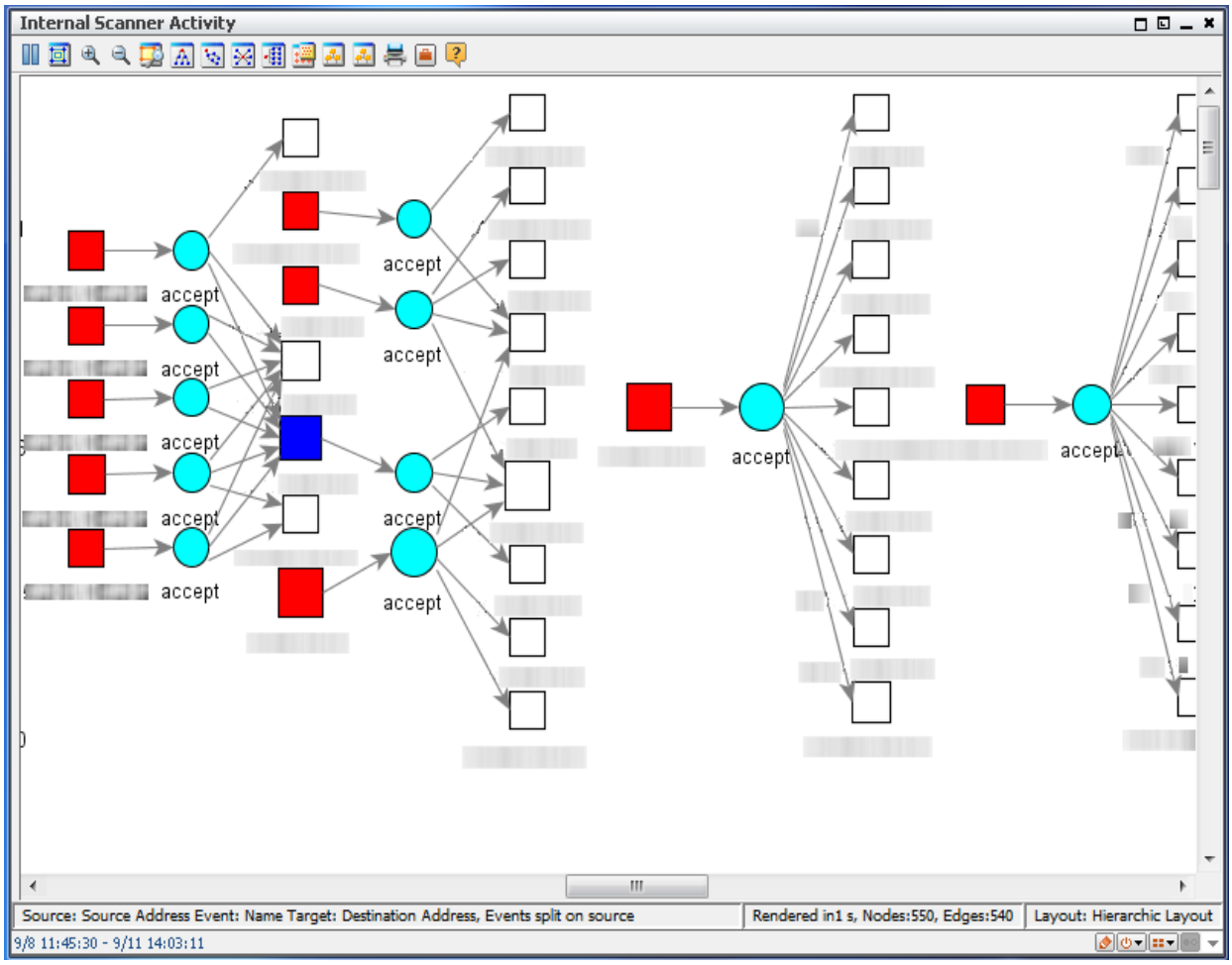


## Using the *Internal Scanner Activity* Data Monitor

The Internal Scanner Activity data monitor tracks scans from internal sources to the destination hosts, all occurring within the network. These hosts reside within the protected address spaces.

The Internal Scanner Activity data monitor is updated every 60 seconds and shows each source that sent a maximum of 1000 scans to protected hosts.

Following is a partial view of the data monitor:




### To view the *Internal Scanner Activity* data monitor:

- On the Reconnaissance use case's Dashboards section, click the link to the dashboard, **Reconnaissance Monitoring**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboard/Downloads/Hostile Activity Detection/Reconnaisance`.
  b. Right-click **Reconnaissance Monitoring** and select **Show Dashboard**.

The Internal Scanner Activity data monitor is displayed on the top right of the Reconnaissance Monitoring dashboard.

### To interpret the *Internal Scanner Activity* data monitor:

- The data monitor uses a hierarchical layout of nodes.
- Red nodes represent scanner (source) addresses.

- Turquoise nodes represent the event name as sent by the device (for example, a firewall might show **permit**, **accept**, or **drop**).
- White nodes represent the hosts' (destinations) addresses.
- Blue nodes can sometimes appear between a red and white squares. A blue node indicates that a chain of scans has occurred, with the blue node as the intermediate scanner.

**Tip:** Try these:

- Zoom in on a particular area especially if the data monitor is displaying many nodes.
- Click the circular layout button (  ) on the toolbar for a different arrangement of the nodes.

### Further investigations on the *Internal Scanner Activity* data monitor:

The activity shown on this data monitor includes routine traffic as well as questionable ones.

- Right-click on a square node (either a source or destination) and choose **Show Events**.
  The Console displays the Internal Scanner Activity active channel, with end time evaluated hourly. Use this channel to determine information about the specific node.
- Right-click on a circle (an event name) and choose **Show Events**.
  The circle represents the event name. If you chose to show events on a specific event name, you can use the information on the Internal Scanner Activity active channel to determine source addresses of internal scanners.

  Refer to the following topics in the *ArcSight Console User's Guide* :
  - The "Reference Guide" section for descriptions of the different categories displayed on the active channel
  - The "Investigating Views" topic for various ways to use the right-click **Investigate** option
- Focus on the source addresses (the internal scanners). Are those scanners authorized to access the destination? For the unauthorized internal scanners, who are the users assigned to those internal scanners?

### To fine tune the *Internal Scanner Activity* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

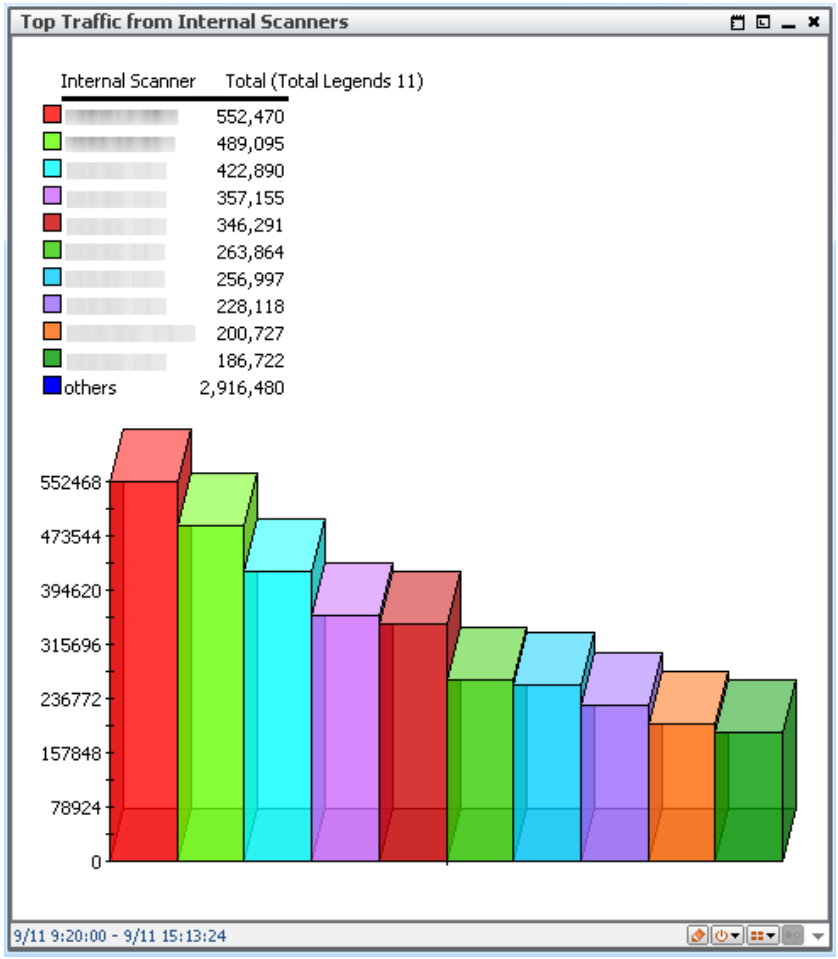
**Caution:** If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

| | |
|---|---|
| Data monitor | • **Availability Interval:** Default is 60 seconds in which the data monitor is updated. You can increase or reduce this number.<br>• **Max Event Count:** Default is 1000 scans. You can increase or decrease the number depending on investigative needs.<br>To edit the data monitor, click the pencil icon ( ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel.<br>The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Event Graph Data Monitor" for details. |
| Filter used by the data monitor | Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Reconnaissance/Internal Scanner Hosts`.<br>**Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter.<br>Refer to the *User's Guide*'s topic on "Filtering Events" for details. |

# Using the *Top Traffic from Internal Scanners* Data Monitor

This data monitor shows the internal sources that generated the most scans in the last 6 hours. The data monitor is updated every 60 seconds.

Following is a closeup of the data monitor.




### To view the *Top Traffic from Internal Scanners* data monitor:

- On the Reconnaissance use case's Dashboards section, click the link to the dashboard, **Reconnaissance Monitoring**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboard/Downloads/Hostile Activity Detection/Reconnaissance`.
  b. Right-click **Reconnaissance Monitoring** and select **Show Dashboard**.

The Top Traffic from Internal Scanners data monitor is located on the bottom center of the dashboard. Use this data monitor to get an overview of the most active internal scanners within your network.

### To interpret the *Top Traffic from Internal Scanners* data monitor:

- Each vertical bar on the chart represents one internal scanner, with the leftmost bar representing the scanner that generated the most traffic.

- By default, the data monitor displays the top 10 internal scanners. The legend shows the total events per scanner with the highest number on top. The legend labeled "others" is a sum of events from the remaining scanners not belonging to the top 10.

### Further investigations on the *Top Traffic from Internal Scanners* data monitor:

Use this data monitor to determine the internal scanners suspected of actively checking hosts for vulnerabilities. This could indicate that these scanners have been compromised and may be even be used to launch real attacks.

- Double-click on a chart element on the graph to open a channel specific to that element. Or right-click an element and choose **Investigate**. Then choose an option to suit your investigative needs.

  **Tip:** Refer to the following topics in the *ArcSight Console User's Guide* :

  - The "Reference Guide" section for descriptions of the different categories displayed on the active channel
  - The "Investigating Views" topic for various ways to use the right-click **Investigate** option

### To fine tune the *Top Traffic from Internal Scanners* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

**Caution:** If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

| | |
|---|---|
| Data monitor | • **# top entries:** Default is 10 top internal scanners. You can increase or reduce this number.<br>• **Bucket size in Seconds:** Default is 600 seconds (10 minutes) per bucket. You can increase or decrease the size depending on investigative needs.<br>• **Number of Buckets:** The default is 36 buckets, which means a time range of 360 minutes or 6 hours. You can increase or decrease the number depending on investigative needs.<br>**Note:** If you want to change the time range of the data monitor, adjust the bucket size or number of buckets, or both.<br>To edit the data monitor, click the pencil icon (  ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel.<br>The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details. |
| Filter used by the data monitor | Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Reconnaissance/Internal Scanner Hosts`.<br>**Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter.<br>Refer to the *User's Guide*'s topic on "Filtering Events" for details. |

# Chapter 7: Monitoring Scanned Hosts

This chapter provides information about critical hosts in your network that are being scanned for reconnaissance purposes.

The following topics are covered:



## Using the *Critical Hosts Scanned* Data Monitor

The Critical Hosts Scanned data monitor tracks, in real time, assets in your network that were scanned, either by external or internal sources. Specifically, these assets have a System Asset Category setting of either **Very High** or **High** criticality.

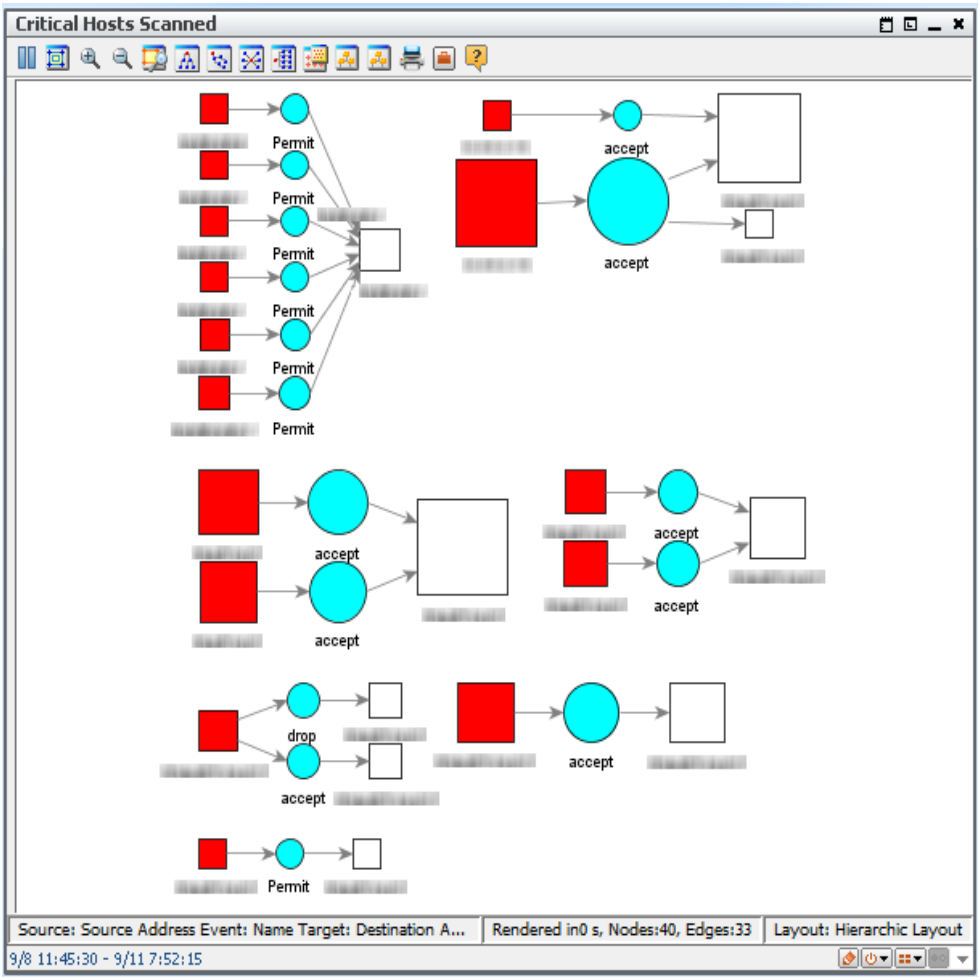
**Tip:** An asset in your network model can be assigned various category settings. The hosts (assets) displayed on this data monitor would have one of these system asset category settings:

- `/All Asset Categories/System Asset Categories/Criticality/Very High`
  or
- `/All Asset Categories/System Asset Categories/Criticality/High`

The above settings are found in an asset's **Categories** tab.

The data monitor is updated every 60 seconds and shows each critical host that was scanned a maximum of 1000 times.

Following is a closeup of the data monitor:




### To view the *Critical Hosts Scanned* data monitor:

- On the Reconnaissance use case's Dashboards section, click the link to the dashboard, **Reconnaissance Monitoring**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboard/Downloads/Hostile Activity Detection/Reconnaissance`.
  b. Right-click **Reconnaissance Monitoring** and select **Show Dashboard**.

The **Critical Hosts Scanned** data monitor is displayed on the top left of the Reconnaissance Monitoring dashboard .

### To interpret the *Critical Hosts Scanned* data monitor:

Red squares represent external source addresses; turquoise circles represent the event name as sent by the device (for example, a firewall might send **Permit**, **accept**, or **drop** events); and white squares

represent the destination addresses of critical hosts in your network. On the top left of the example, you can see multiple sources targeting a single critical host.

### Further investigations on the *Critical Hosts Scanned* data monitor:

Use this data monitor to determine which critical assets and their zones are of interest to the scanners.

- Right-click on a square node (either a source or destination) and choose **Show Events**.

  The Console displays the Critical Hosts Scanned active channel, with end time evaluated hourly. Use this channel to determine information about the specific node. For example, if you chose to show events on a white node (the critical host destination), the active channel displays all incoming events on that host.

- Right-click on a circle (an event name) and choose **Show Events**.

  The circle represents the event name. If you chose to show events on an **accept** event, you can use the information on the Critical Hosts Scanned active channel to determine source addresses whose scans were accepted by critical hosts. The channel displays information about the sources such as their zones, countries, and so on.

  **Tip:** Refer to the following topics in the *ArcSight Console User's Guide* :

  - The "Reference Guide" section for descriptions of the different categories displayed on the active channel
  - The "Investigating Views" topic for various ways to use the right-click **Investigate** option

### To fine tune the *Critical Hosts Scanned* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

**Caution:** If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

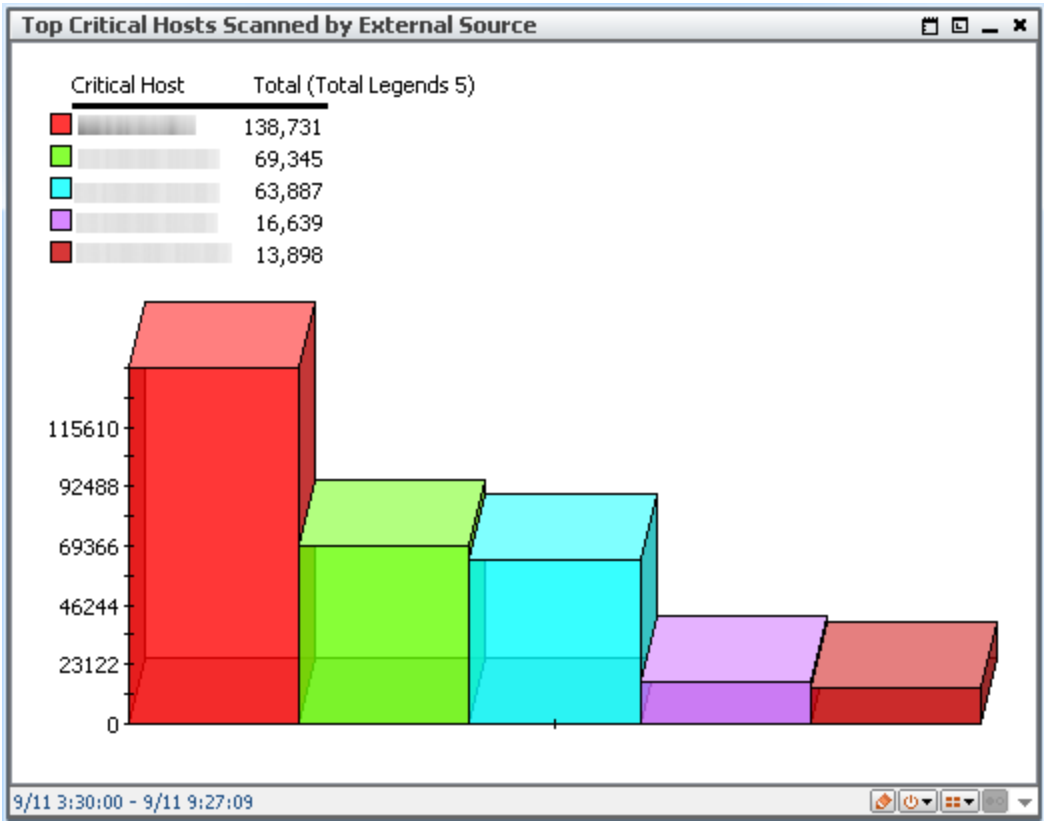
| | |
|---|---|
| Data monitor | • **Availability Interval:** Default is 60 seconds in which the data monitor is updated. You can increase or reduce this number.<br>• **Max Event Count:** Default is 1000 scans. You can increase or decrease the number depending on investigative needs.<br>To edit the data monitor, click the pencil icon ( ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel.<br>The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Event Graph Data Monitor" for details. |
| Filter used by the data monitor | Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Reconnaissance/Critical Assets Scanned`.<br>**Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter.<br>Refer to the *User's Guide*'s topic on "Filtering Events" for details. |

# Using the *Top Critical Hosts Scanned by External Source* Data Monitor

This data monitor tracks the top critical assets that were scanned by external sources. While it is impossible to control external sources, with this data monitor, you have the ability to protect those critical assets before a real attack comes.

The data monitor shows the top 10 critical hosts that were scanned a maximum of 1000 times. Information is updated every 60 seconds.

Following is a closeup of the data monitor:




### To view the *Top Critical Hosts Scanned by External Source* data monitor:

- On the Reconnaissance use case's Dashboards section, click the link to the dashboard, **Reconnaissance Monitoring**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboard/Downloads/Hostile Activity Detection/Reconnaissance`.
  b. Right-click **Reconnaissance Monitoring** and select **Show Dashboard**.

The **Top Critical Hosts Scanned by External Sources** data monitor is displayed on the bottom left of the Reconnaissance Monitoring dashboard.

### To interpret the *Top Critical Hosts Scanned by External Source* data monitor:

The vertical bars display the critical hosts with very high scan counts from outside sources. The host with the highest count is on the left.

### Further investigations on the *Top Critical Hosts Scanned by External Source* data monitor:

Use this data monitor to determine which critical assets are being scanned the most, by external sources.

- Double-click a chart element on the graph to open an active channel specific to that element. Or right-click a chart element and choose **Investigate**, then choose an option to suit your investigative needs.

  Refer to the following topics in the *ArcSight Console User's Guide* :
  - The "Reference Guide" section for descriptions of the different categories displayed on the active channel
  - The "Investigating Views" topic for various ways to use the right-click **Investigate** option

### To fine tune the *Top Critical Hosts Scanned by External Sources* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

**Caution:** If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for details.

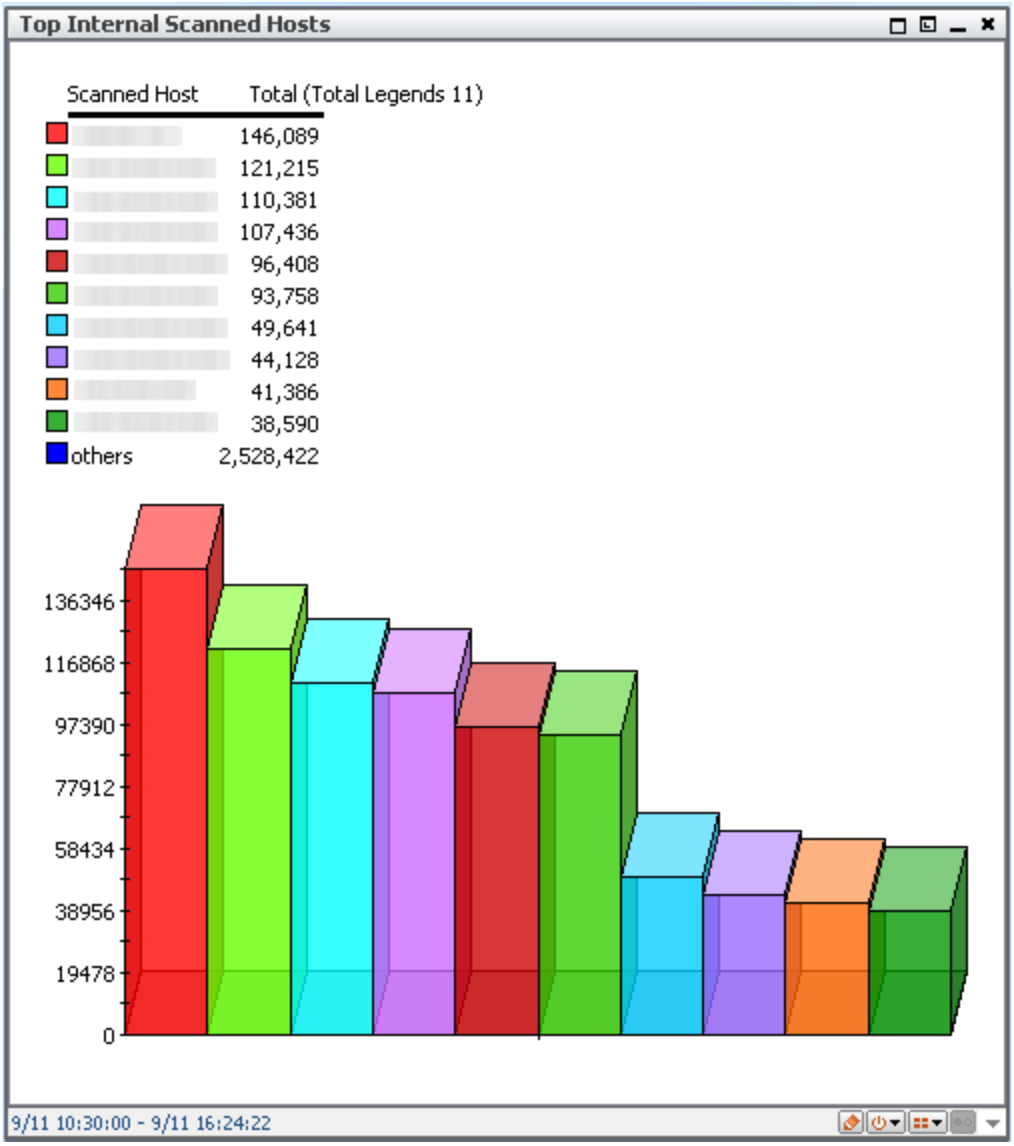
| | |
|---|---|
| Data monitor | • **# of top entries:** Default is top 10 critical hosts. You can increase or reduce this number.<br>• **Bucket size in Seconds:** Default is 600 (10 minutes) per bucket. You can increase or decrease the size depending on investigative needs.<br>• **Number of Buckets:** The default is 36 buckets, which means a time range of 360 minutes or 6 hours. You can increase or decrease the number depending on investigative needs.<br>**Note:** If you want to change the time range of the data monitor, adjust the bucket size or number of buckets, or both.<br>To edit the data monitor, click the pencil icon (  ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel.<br>The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details. |
| Filter used by the data monitor | Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Reconnaissance/Critical Assets Scanned by External Sources`.<br>**Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter.<br>Refer to the *User's Guide*'s topic on "Filtering Events" for details. |

# Using the *Top Internal Scanned Hosts* Data Monitor

This data monitor shows the internal scanned hosts sorted by traffic coming from external or internal scanners within the last 6 hours. It provides an overview of the most recent reconnaissance activity against the network.

The data monitor shows the top 10 internal hosts that were scanned a maximum of 1000 times. Information is updated every 60 seconds.

Following is a closeup of the data monitor:



### To view the *Top Internal Scanned Hosts* data monitor:

- On the Reconnaissance use case's Dashboards section, click the link to the dashboard, **Reconnaissance Monitoring**.

  Or

- On the Navigator > Resources panel:
  a. Go to `/All Dashboard/Downloads/Hostile Activity Detection/Reconnaissance`.
  b. Right-click **Reconnaissance Monitoring** and select **Show Dashboard**.

The data monitor is located on the bottom right of the dashboard. Use this data monitor to investigate what scanners consider to be the top "most popular" hosts.

### To interpret the *Top Internal Scanned Hosts* data monitor:

- Each vertical bar on the chart represents one internal scanned host, with the leftmost bar representing the host that received the most traffic.
- By default, the data monitor displays the top 10 internal scanned hosts. The legend shows the total events per host with the highest number on top. The legend labeled "others" is a sum of events from the remaining scanned hosts not belonging to the top 10.

### Further investigations on the *Top Internal Scanned Hosts* data monitor:

Use this data monitor to identify the applications installed in the internally scanned hosts. Are these applications critical to your operations? What is the impact if such hosts are attacked?

- Double-click a chart element on the graph to open a channel about that element. Or right-click a chart element and choose **Investigate**, then choose an option to suit your investigative needs.

  Refer to the following topics in the *ArcSight Console User's Guide* :
  - The "Reference Guide" section for descriptions of the different categories displayed on the active channel
  - The "Investigating Views" topic for various ways to use the right-click **Investigate** option
- Right-click on an event and select **Export**. Then select one of the available export options. Refer to the *ArcSight Console User's Guide*'s topic, "Exporting Events to a File," for more information.

### To fine tune the *Top Internal Scanned Hosts* data monitor:

ArcSight ESM provides filters to refine the data returned by the data monitor. The data monitor itself has default parameters that determine the time buckets.

**Caution:** If making changes to any parameters, you must be familiar with factors that affect ESM performance resulting from these changes. You must also know how to edit ESM resources, such as modifying filter conditions and other attributes. Refer to the *ArcSight Console User's Guide* for

details.

| | |
|---|---|
| Data monitor | • **# top entries:** Default is 10 top internal scanned hosts. You can increase or reduce this number.<br>• **Bucket size in Seconds:** Default is 600 seconds (10 minutes) per bucket. You can increase or decrease the size depending on investigative needs.<br>• **Number of Buckets:** The default is 36 buckets, which means a time range of 360 minutes or 6 hours. You can increase or decrease the number depending on investigative needs.<br>**Note:** If you want to change the time range of the data monitor, adjust the bucket size or number of buckets, or both.<br>To edit the data monitor, click the pencil icon ( ) on the bottom toolbar of the data monitor. This opens the data monitor's Edit panel.<br>The attributes of this data monitor type are described in the *ArcSight Console User's Guide*'s topic on "Top Value Counts Data Monitor" for details. |
| Filter used by the data monitor | Change the filter conditions to suit your business requirements. The filter is located in `/All Filters/Downloads/Hostile Activity Detection/Reconnaissance/Internal Scanned Hosts`.<br>**Caution:** Before modifying any filter, verify if this filter is being used by other resources. Changes to filter conditions will affect the expected results in all resources using the filter.<br>Refer to the *User's Guide*'s topic on "Filtering Events" for details. |

# Chapter 8: Refining the *Reconnaissance from Internal Sources* Rule

The Reconnaissance security use case includes multiple rules to set event fields with values relevant to tracking Reconnaissance activities. You are not required to modify these rules.

You can, however, modify the rule called **Reconnaissance from Internal Source** in `/All Rules/Downloads/Hostile Activity Detection/Reconnaissance`. By default, this rule is designed to add information about the source (scanner) address, the source zone, and customer data to the **Internal Scanners** and **Scanners List** active lists.

Additionally, the rule has the following default but *disabled* actions:

- Create a case in `/All Cases/Downloads/Hostile Activity Detection/Reconnaissance`. with the following features:
  - The case name is `Reconnaissance from Internal Source <source ip address> Detected`
  - Include the base events related to the case.

    **Note:** If the case does not yet exist, the rule first creates the case with the dynamically-configured name then adds the base events to it. When the rule is triggered in the future, new base events are added to the case.
- Send notification about the scan to the default destination, `/All Destinations/SOC Operators/`.
  - If you want to enable this rule with the default destination, make sure to configure it by adding users to the appropriate destination levels.
  - If you want to enable this rule action and you are not using the default destination `SOC Operators`, make sure you first define your own destination resource. Then specify your custom destination to the rule action.

  Refer to the "Managing Notification Destinations" in the *ArcSight Console User's Guide*.

### To customize rule actions:

**Tip:** Refer to the *ArcSight Console User's Guide*'s topic on "Rule Actions Reference" for details on the rule actions described here.

1. Log into the ArcSight Console with administrator privileges.
2. Go to `/All Rules/Downloads/Hostile Activity Detection/Reconnaisance`, right-click **Reconnaissance from Internal Source**, and choose **Edit Rule**.

3. Click the disabled rule action, **Add To Existing Case**.
   a. On the **Actions** tab, right-click and choose **Enable Action**.
   b. If you want to further modify the rule action, right-click again and choose **Edit**.

      For example, change the `URI` if you have previously created a custom case group for reconnaissance tracking purposes.
4. Click the disabled rule action, **Send Notification**.
   a. Right-click and choose **Enable Action**.
   b. If you want to modify the rule action further, right-click again and choose **Edit**.

      For example, choose a different destination group and customize the notification message.

# Send Documentation Feedback

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

**Feedback on Security Use Case Guide (ESM: Reconnaissance 1.0)**

Just add your feedback to the email and click send.

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

We appreciate your feedback!