Hewlett Packard
Enterprise

HPE Security ArcSight ESM: IDS - IPS Monitoring

Software Version: 1.0

Security Use Case Guide

June 17, 2016

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

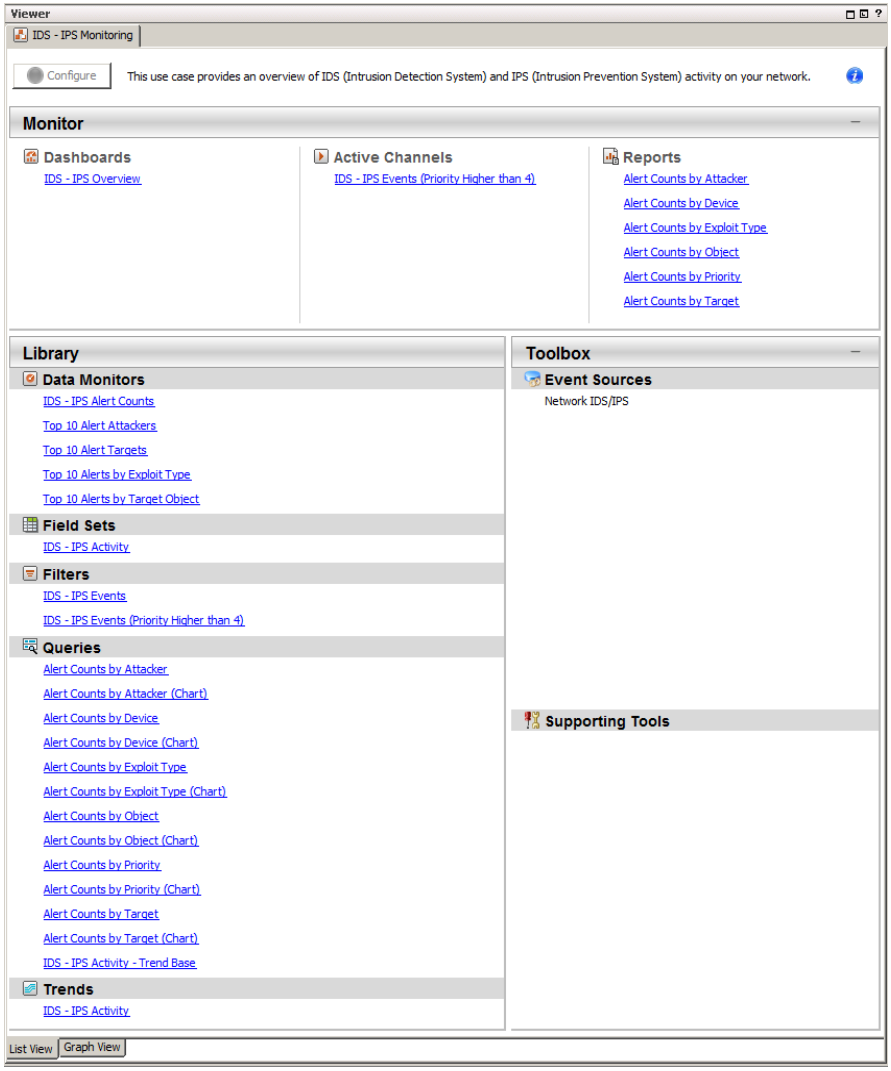
The IDS - IPS Monitoring use case provides an overview of the network activity identified by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), showing a real-time awareness of your network situation through an active analysis of IDS and IPS events that identify suspicious patterns. These patterns might indicate a network or system attack from someone attempting to break into or compromise a system.

Use the resources in this use case for incident investigation as well as routine monitoring and reporting to see what type of activity is being detected, such as unusual behavior, abnormal traffic, or malicious coding.

- A **dashboard** is provided to show an overview of IDS and IPS alerts in real time.
- An **active channel** is provided so that you can investigate IDS and IPS events that have an ESM priority rating higher than 4, which indicates a potential concern.
- Several **reports** provide charts and tables showing the number of alerts by exploit type, device, target, attacker, object, and ESM priority. The reports are based on a **trend** that collects daily information about IDS and IPS activity.

You can access the IDS - IPS Monitoring use case from the **Use Cases** tab of the ArcSight Console Navigator panel. The Monitor section of the use case lists the dashboard, active channel, and reports used to monitor traffic and investigate events. The Library section of the use case lists all supporting resources that help compile information in the dashboard, active channel, and reports.

The IDS - IPS Monitoring use case is shown below.



This document describes how to install, configure, and use the IDS - IPS Monitoring 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 ArcSightESM help system from the ArcSight Console **Help** menu. Find PDFs of all ArcSight documentation on Protect 724.

Chapter 2: Installation

To install the IDS - IPS Monitoring use case, perform the following tasks in the following sequence:

1. Download the IDS - IPS Monitoring use case zip file into the ArcSight Console system where you plan to install the use case, then 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 IDS - IPS Monitoring use case package. See "Importing and Installing a Package" on the next page for details.
6. Assign user permissions to the IDS - IPS Monitoring resources. See "Assigning User Permissions" on page 8 for details.

No configuration is required for the IDS - IPS Monitoring use case. However, before using the IDS - IPS Monitoring use case, make sure that you have populated your ESM network and asset models. A network model keeps track of the network nodes participating in the event traffic. Assets provide more granular attributes of the nodes, such as descriptions of critical servers. For information about populating the network model, refer to the *ArcSight Console User's Guide*.

Importing and Installing a Package

Follow the steps below to import and install the package(s). This assumes you have downloaded the zip file and extracted the contents into the ArcSight Console system.

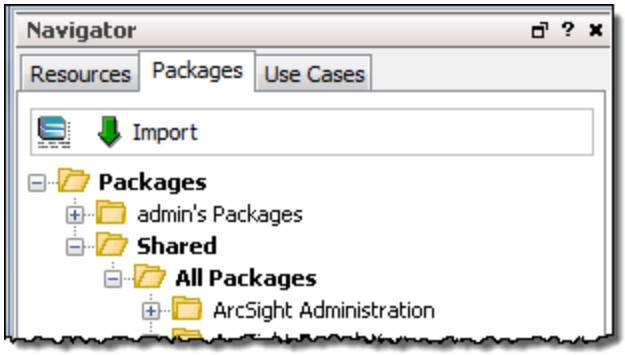
- If the ArcSight Console does not have the Downloads Groups package in `/All Packages/Downloads/Downloads Groups`, import and install the package first. Then repeat the steps to import and install the **IDS - IPS Monitoring** use case package.

  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 IDS - IPS Monitoring 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 package file (`*.arb`) 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 the resources. Users in the `Default User Groups` (and any custom user group under this group) can only view IDS - IPS Monitoring 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 right 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 right users.

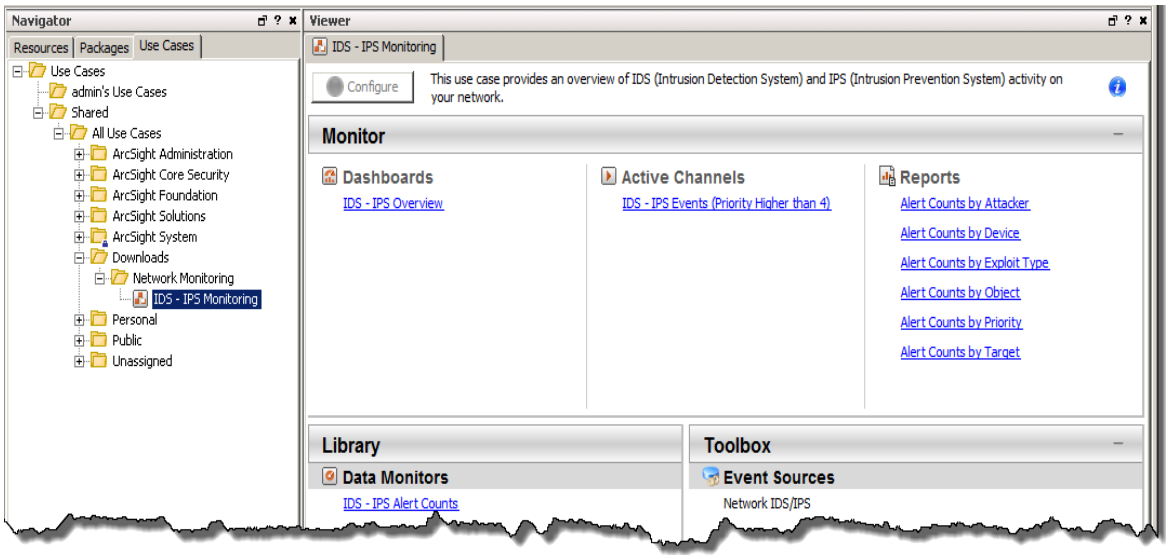
To assign user permissions:

1. In the Navigator panel, open the **Resources** tab.
2. For each of the resource types provided in the use case, navigate to `Downloads/IDS - IPS Monitoring`.
3. Right-click the `IDS - IPS Monitoring` 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: Using the IDS - IPS Monitoring Use Case

The IDS - IPS Monitoring use case is located on the **Use Cases** tab in the Navigator panel under `/All Use Cases/Downloads/Network Monitoring`.

To open the IDS - IPS Monitoring use case in the Viewer panel, either double-click the use case or right-click the use case and select **Open Use Case**.



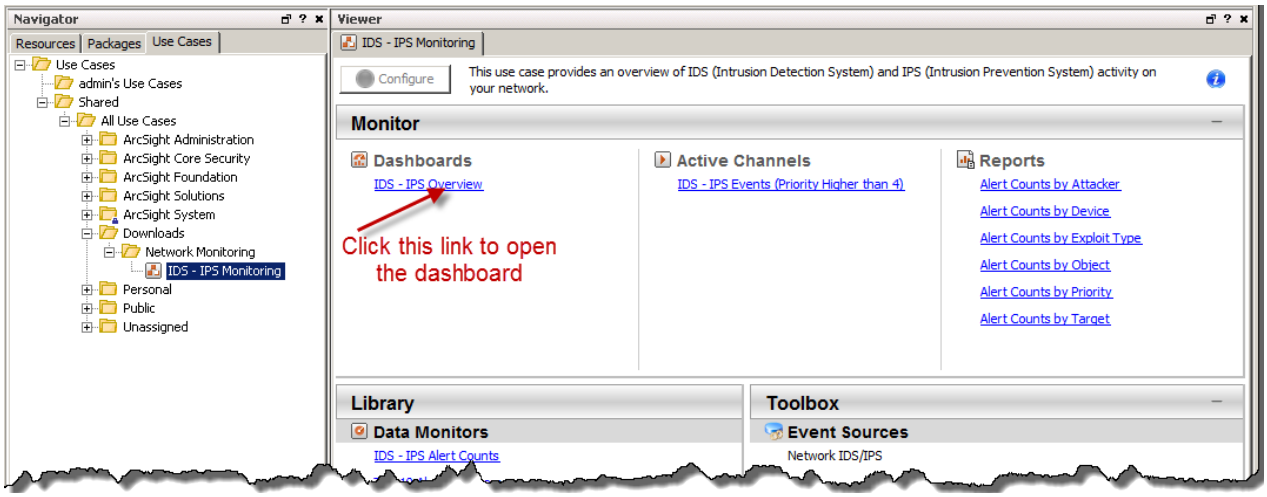
The Monitor section of the IDS - IPS Monitoring use case provides resources to help you monitor and investigate IDS and IPS traffic:

- Use the dashboard to monitor IDS - IPS alerts in real time. See "Monitoring IDS and IPS Alerts in a Dashboard" on the next page.
- Use the active channel to investigate priority IDS and IPS events. See "Investigating Priority Events in an Active Channel" on page 13.
- Run reports that show the number of alerts by device, target, object, exploit type, priority, and attacker in chart or table format. "Running Reports" on page 15.

Monitoring IDS and IPS Alerts in a Dashboard

The IDS - IPS Monitoring use case provides a dashboard to help you monitor all IDS and IPS alerts in real time so that you can identify the most important threats facing your network and any anomalies that need investigation. You can see the top ten exploit types, attackers, targets, and target objects (such as a database or an application) reported by your IDS and IPS, and the top ten alert counts with an ESM priority higher than 4. Understanding the top exploit types, and the most frequent attackers and targets enables you to investigate and remediate potential threats before they can damage your network.

To open the **IDS - IPS Overview** dashboard, click the link for dashboard in the IDS - IPS Monitoring use case.



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

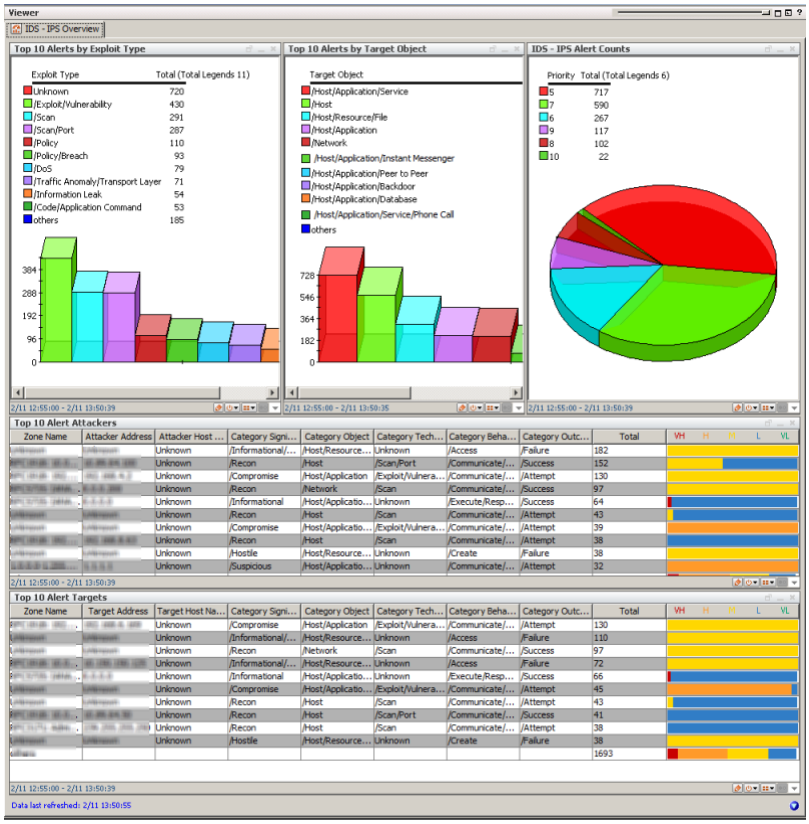
The **IDS - IPS Overview** dashboard provides the following data monitors:

- **Top 10 Alerts by Exploit Type** shows the most frequent exploit types being used to attack your network, such as SQL injections, information leaks, and cross-site scripting. Understanding the exploit types affecting your network enables you to mitigate significant security risks and put procedures in place to protect the network.
- **Top 10 Alerts by Target Object** shows the most frequent IDS alerts grouped by target object. A target object can be an application, the operating system, a database, a file system, or the memory of a server. This is the object that is being accessed or altered. If there is a high number of alerts for a specific target that is a sensitive asset on your network (for example, a system that has restricted or internal data), there might be an exploit in progress and you should investigate promptly.
- **IDS - IPS Alert Counts** shows the number of IDS and IPS alerts grouped by priority (higher than 4). The ESM priority rating is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. A high priority generally indicates an event with

a high risk factor. Whereas an event with a priority of 5 or 6 indicates a potential concern, such as pre-attack scan activity or policy violation, an event with a priority of 8 or 9 is a grave concern and might indicate that there is an exploit in progress, such as an SQL injection, information leak, or cross-site scripting.

- **Top 10 Alert Attackers** shows the IP addresses of the attackers (assets from which an attack originates) with the most alerts. Knowing the attackers helps you understand the intent of the attacks and how they affect the assets on your network.
- **Top 10 Alert Targets** shows the IP addresses of the targets (assets that are the intended focal point of an alert) with the most alerts. These targets can be sensitive assets on your network that need to be protected.

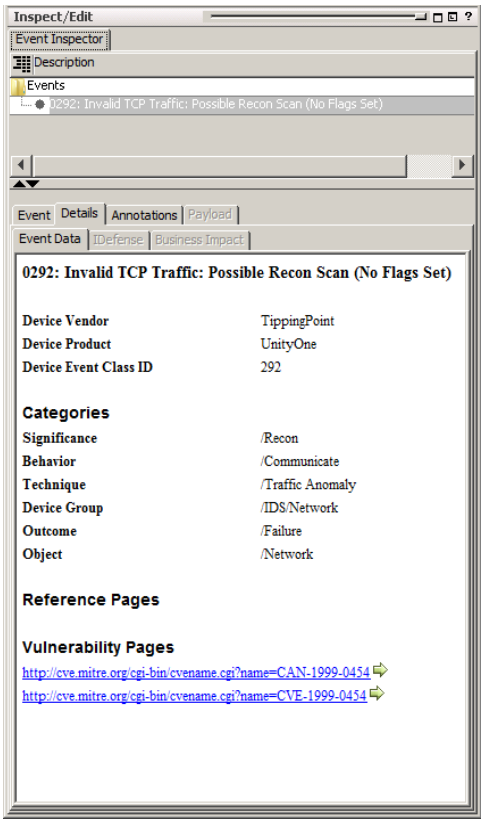
An example dashboard is shown below.



Right-click on an item in a data monitor and select **Investigate > Create Channel** to open an active channel and investigate further. For example, right-click on an exploit type in the **Top 10 Alerts by Exploit Type** data monitor and select **Investigate > Create Channel** to open an active channel and investigate the exploit to obtain details about the attacker IP address and the target IP address. In the active channel, you can also:

- Create an inline filter to focus on events of interest; for example, attacks received by a sensitive asset on your network, such as a DNS server or a domain controller. For detailed information about using inline filters, see the *ArcSight Console User's Guide*.
- Double-click on an event in the active channel to open the event inspector and see details about the

event. The example below shows the Details tab of the Event Inspector for an invalid TCP traffic event, and provides the IDS device vendor and product, as well as external links to vulnerability pages that discuss the vulnerability further.



Investigating Priority Events in an Active Channel

The **IDS - IPS Events (Priority Higher than 4)** active channel shows all events from IDS and IPS devices with an ESM priority rating higher than 4. The ESM priority rating is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. HPE recommends that you investigate events with a priority higher than 4 to identify potential malicious activities.

For details about the priority rating and how it is calculated, see the *ArcSight Console User's Guide*.

To open the **IDS - IPS Events (Priority Higher than 4)** active channel, click the link for the active channel in the IDS - IPS Monitoring use case.

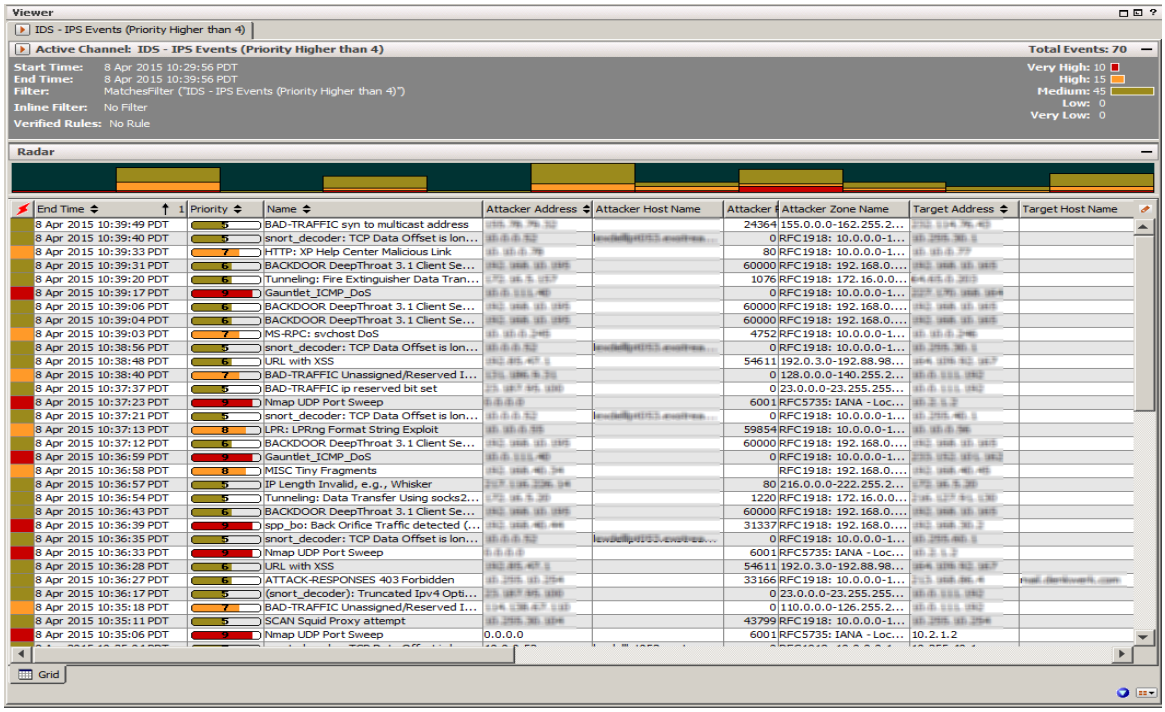
The active channel opens in the Viewer of the ArcSight Console and displays all IDS and IPS events received within the last ten minutes.

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.

An example **IDS - IPS Events (Priority Higher than 4)** active channel is shown below.



The active channel lists all events with an ESM priority higher than 4.

Note: Not every high priority event is necessarily a threat. For example, if IDS alerts are sending false positives from scheduled penetration testing, the priority of the events might be very high, but this does not necessarily represent a threat to your network.

The event priority in the active channel is color coded to help you zone in on potential problems. The table below describes the priority levels you might see.

Priority	Color	Description
5-6	Yellow	**Medium** priority. This event indicates a potential concern, such as pre-attack scan activity, policy violation, and identified vulnerability. Medium priority events are often hostile attempts whose success or failure is not confirmed.
7-8	Orange	**High** priority. This event indicates a concern, such as attack formations, potential breaches, or misuse, including incorrect registry values or a SYNFlood.
9-10	Red	**Very high** priority. This event presents a grave concern, such as a verified breach or a DHCP packet that does not contain enough data. Investigate items with a very high priority immediately because there might be an exploit in progress, such as an SQL injection, information leak, or cross-site scripting.

Use this active channel as a base line for your investigation. Right-click an item (such as 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.

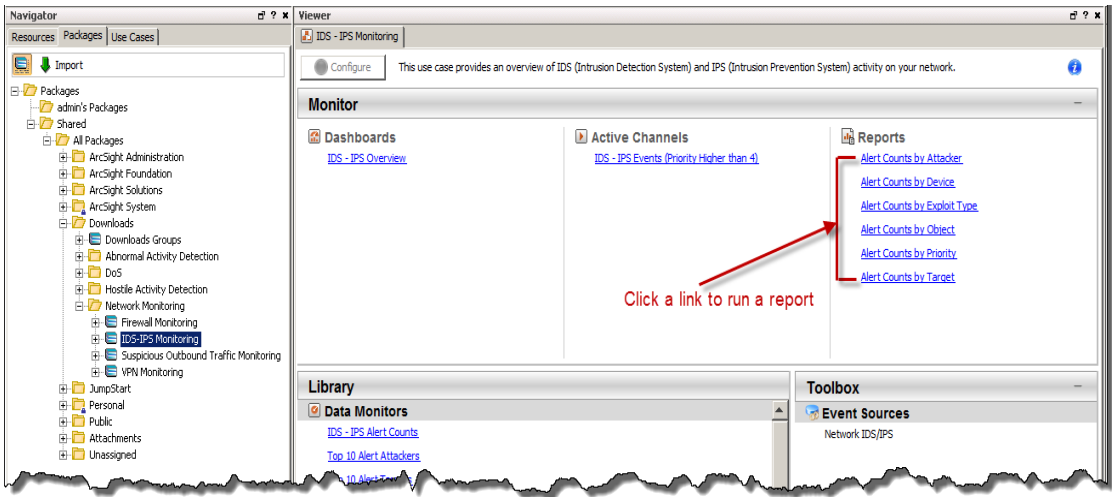
Running Reports

The IDS - IPS Monitoring use case provides several reports that you can run to obtain a historical view of the IDS and IPS situation on your network and provide to the stakeholders in your company, when needed.

By default, the reports use data from the previous day. You can change the start and end time of the report for longer- or shorter-term analysis when you run the report.

To run a report:

1. Click the link for the report in the IDS - IPS Monitoring use case.



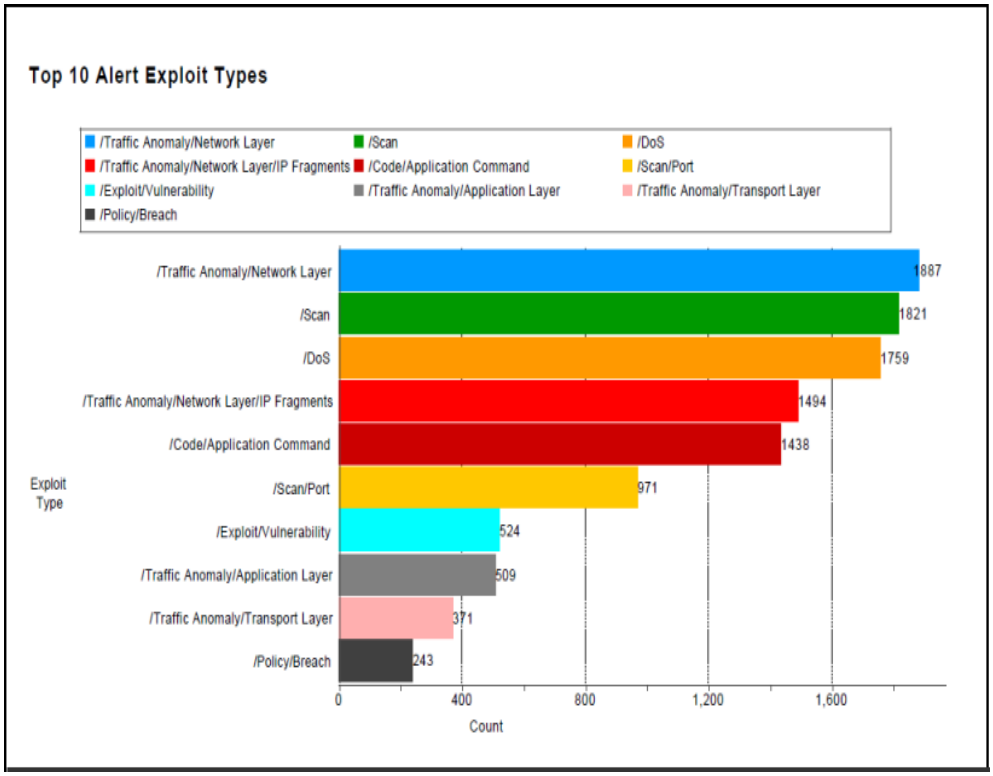
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time.
3. For formats other than HTML, either open the report or save the report to your computer when prompted.

The IDS - IPS Monitoring use case provides the following reports:

- **Alert Counts by Attacker** shows the total number of IDS and IPS alerts by attacker with an ESM priority greater than 4, for the previous day. A chart shows the IP addresses of the top ten attackers. A table shows a list of all attackers with an ESM priority higher than 4. A priority higher than 4 can indicate potential malicious activities. Knowing the attackers helps you understand the intent of the attacks and how they affect the assets on your network.

- **Alert Counts by Device** shows the number of IDS and IPS alerts by device. A chart shows the IP addresses of the top ten devices with the highest number of alerts. A table lists the devices with alerts showing the IP address, vendor and product type of each device.
- **Alert Counts by Exploit Type** shows the number of IDS and IPS alerts by exploit type, such as SQL injections, information leaks, and cross-site scripting. A chart shows the top ten exploit types. A table shows a list of all the exploit types. Understanding the exploit types affecting your network enables you to mitigate significant security risks and put procedures in place to protect the network.
- **Alert Counts by Object** shows the total number of IDS and IPS alerts by object, such as application, operating system, database, file, or server memory. A chart shows the top ten objects with the highest number of alerts. A table shows a list of all the objects. A high number of alerts for a specific object that stores sensitive data on your network (for example, a database that contains restricted data or personal information), might indicate that a serious security breach has taken place.
- **Alert Counts by Priority** shows the total number of IDS and IPS alerts by priority. A chart shows the number of alerts by priority. A table shows the number of alerts with an ESM priority higher than 4. A high priority generally indicates an event with a high risk factor. A priority rating of 9 or 10 is a grave concern and might indicate an important threat, such as an SQL injection, information leak, or cross-site scripting.
- **Alert Counts by Target** shows the total number of IDS and IPS alerts by target with an ESM priority rating higher than 4. A chart shows the top ten target IP addresses. A table shows a list of all the targets with an ESM priority higher than 4. A high number of alerts for a specific target that is a sensitive asset on your network (for example, a system that has restricted or internal data) might indicate a serious security breach.

An example report is shown below.


Top 10 Alert Exploit Types
/Traffic Anomaly/Network Layer
/Scan
/DoS
/Traffic Anomaly/Network Layer/IP Fragments
/Code/Application Command
/Scan/Port
/Exploit/Vulnerability
/Traffic Anomaly/Application Layer
/Traffic Anomaly/Transport Layer
/Policy/Breach
Exploit Type
1887
1821
1759
1494
1438
971
524
509
371
243
0
400
800
1,200
1,600
Count

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: IDS - IPS Monitoring 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!