Hewlett Packard
Enterprise

HPE Security ArcSight Interactive Discovery

Software Version: 6.7.2

Project Guide

November 22, 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 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 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/welcome

Contents

Chapter 1: About ArcSight Interactive Discovery

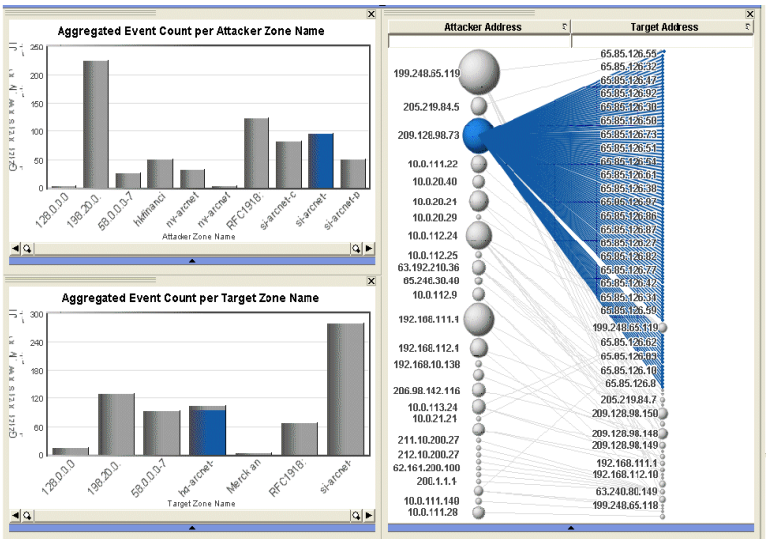
ArcSight Interactive Discovery augments ArcSight Logger and ArcSight Enterprise Security Management's Pattern Discovery, dashboards, reports, and analytical graphics. Interactive Discovery provides enhanced forensic data analysis and reporting capabilities using a comprehensive selection of pre-built interactive statistical graphics.

Use Interactive Discovery to:

- Quickly gain insight into your complex security data
- Explore and drill down into security data with unprecedented control and flexibility
- Accelerate discovery of hard to find, suspicious events
- Present state of security in compelling visual summaries
- Build a persuasive, non-technical call to action
- Prove IT Security value and help justify budgets

How Interactive Discovery Works

With flat data in a table it is hard to tell which events are significant and how one may relate to another. But Interactive Discovery can display data points in relation to each other in meaningful and business-applicable ways, so that you can see that, for example, one attacker with many failed connections to targets could indicate a port scan or a worm.



Interactive Discovery visualizes data exported from reports and filters in the Logger and ESM Content Packs. These reports provide the formatted event data for Interactive Discovery to visualize.

Interactive Discovery can also visualize data exported from ArcSight Logger using either search and export or ArcSight Logger reports. The search queries and reports are provided in the ArcSight Logger Interactive Discovery Content Pack.

ArcSight Interactive Discovery enables you to learn new things about your network security activity. During daily human analysis of the past day's data, you may find new things that were missed by the analyst. You can use this data to build new rules that improve your overall enterprise security management process.

This guide describes the ArcSight project files. For information on using ArcSight Interactive Discovery, use the online help system accessible from the user interface.

Audience

This guide is intended for ArcSight ESM or ArcSight Logger users who wish to use the advanced analysis and graphics capabilities of Interactive Discovery.

To effectively use ArcSight Interactive Discovery, you should have knowledge of:

- Your network security architecture, protocols, and outputs
- Basic principles of data and statistical analysis

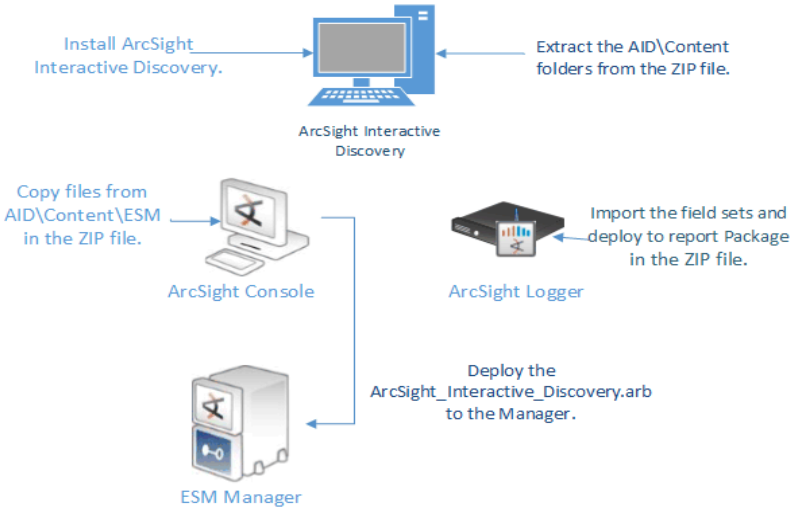
Chapter 2: Installing Interactive Discovery

Before installing Interactive Discovery, first familiarize yourself with Interactive Discovery's deployment architecture and evaluate the system requirements.

Installation Overview

ArcSight Interactive Discovery can be resource-intensive when operating on large files, so it is recommended that you install it on its own host. If you have systems with large RAM capacities (2 or more GB), you can deploy Interactive Discovery on the same system that hosts the ArcSight Console.

The installation consists of several parts, all contained in the downloaded `AID_6.7.2.zip` file.



- Install the program (32-bit or 64-bit) from the ZIP file onto the system that will run Interactive Discovery.

  Note: The *ADVIZOR Implementation Guide* recommends 64 bit.

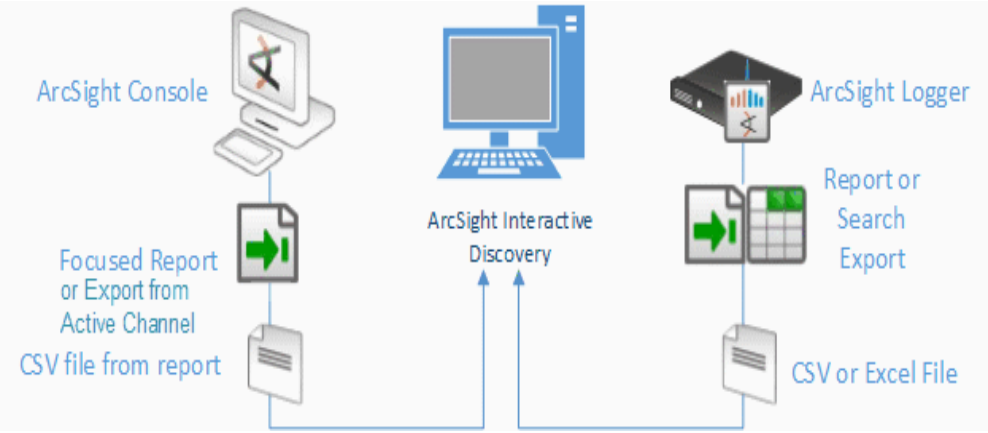
- Extract the ArcSight Interactive Discovery project files directory onto the Interactive Discovery system.
- Deploy the ArcSight_Interactive_Discovery.arb to the Manager.
- Import the Field Sets and deploy the reports to the Logger.

Run the installation on the Interactive Discovery system.

Operations Overview

Place the Interactive Discovery project files with the file extension adv on the Interactive Discovery system. These project files contain a data source reference to the CSV data file that you export from

ESM or Logger. The data itself is not contained in the ADV file, rather, the ADV file refers to the data in the CSV file. When you open a project ADV file, it reads the data from the CSV file source.



The ArcSight Console is the host system for the ArcSight Focused Report or the Export from Active Channel which both create the .CSV file for use by the AID .ADV template. In Logger you generate a report and save it to a CSV file for import into AID. You can also use one of the included fieldsets to perform a Logger search save it to a CSV file. Copy the CSV file to the Interactive Discovery system.

If you share projects among users with different Interactive Discovery instances on different systems, either send them the project file and the data source file, or provide users with a shared network directory where the files are located on a central Interactive Discovery system. You can also share the combined data and template in a .ADVM file which combines the compressed data with the template for a simple one file format.

The AID schema contains event fields that ArcSight considers to be the most common event fields to evaluate for most security situations and reduces the data to process.

Note: A large schema (dozens of columns) and large return sets (millions of rows in a single query) can cause a performance impact on ESM and Logger. To minimize this, ArcSight recommends that when you create your search criteria, that you be as specific as your use case permits.

What's in the Download

The Interactive Discovery download file is `AID_6.7.2.zip`. It contains a number of files, many of which the installer uses. When you unzip this file, the content of these folders is described below.

Content from these folders are used during installation:

- `AID_6.7\Advizor`: the AID installer, "`ArcSight Interactive Discovery Bundle.exe.`", in both 32-bit and 64-bit files, as well as the *Advizor Implementation Guide* and release notes.
- `AID_6.7\Content\ESM`: the ESM content pack, sample data, and project files. **Do not change these files in any way.**

- `AID_6.7\Content\Logger` : the ArcSight Logger content pack, sample data, and project files. **Do not change these files in any way.**
- `AID_6.7\HP_Data_Analysis\ESM` (and `\Logger`) these are working copies of the files in the `AID_6.7\Content folder` . This is your **work area**.

The `AID_6.7\Content\ESM` folder contains the following files:

File	Description
AID_Schema.csv	The project `ArcSight_AID_Schema.adv` uses this file as its data source. As delivered this is a sample data file that contains the AID schema of data output. After installation, you can use it to test the functions of ArcSight Interactive Discovery. Later, when you generate real CSV data files, you can save them with different names. ADV projects allow you to select different CSV data source files and then you can save your projects with different names for different CSV files.
AID_Schema.ini	The INI file that contains initialization settings for the CSV data source file of the same name. This file name must match the name of the CSV file your ADV file uses, so if you rename or create a new CSV file, rename or create a copy of an INI file for it. Place the INI file in the same folder as its CSV file.
ArcSight_AID_ Schema.adv	An AID project file for ESM, that utilizes the AID_Schema (dataset) in Interactive Discovery
ArcSight_AID_ Schema.backup	Backup of the corresponding file. Created automatically.
ArcSight_AID_ Schema_ Business_ Role.advm	Self-contained sample project file, used for familiarization with the product.
ArcSight_ Interactive_ Discovery.arb	You copy this ArcSight package file to the ESM Console, from which you import it to the ESM Manager. The ARB file contains the reports, filters, and focused reports required to output data for consumption by Interactive Discovery. The content of the ARB is described in "ESM Focused Reports " on page 16.
PriorityByBin.asl	Enables color sorting by ArcSight ESM Active Channel Priority.

The `AID_6.7\Content\Logger` folder contains the following files:

File	Description
Logger_AID_ Schema.adv	An AID project file for Logger, that utilizes the AID_Schema (dataset) in Interactive Discovery
Logger_AID_ Schema.backup	Backup of the corresponding file. Created automatically.
Logger_AID_ Schema.advm	Included for demonstration scripts. Any .adv file can be imported and then exported as .advm. The data is NOT refreshed from the source unless the user forces it to do so. Additionally, the .advm file is much smaller than the .adv and .csv combined, as it is already compressed.
Logger_AID_ Schema.csv	The project uses this file as its data source. As delivered this is a sample data file that contains the AID_Schema of data output. After installation, you can use it to test the functions of ArcSight Interactive Discovery. Later, when you generate real CSV data files, you can save them with different names. ADV projects allow you to select different CSV data source files and then you can save your projects with different names for different CSV files.
Logger_AID_ Schema.ini	The INI file that contain initialization settings for the CSV data source file of the same name. This file name must match the name of the CSV file your ADV file uses, so if you rename or create a new CSV file, rename or create a copy of an INI file for it. Place the INI file in the same folder as its CSV file.
Logger_AID_ Schema_ Report.csv	Sample file shipped with the product. Used by the Logger_AID_Schema.adv file provided. To use a sample file, copy the file and rename it to match the corresponding default CSV file in the `\AID_6.7\HP_Data_Analysis\Logger` subdirectory.
Logger_AID_ Schema_ Search.csv	Sample file shipped with the product. Used by the Logger_AID_Schema.adv file provided. To use a sample file, copy the file and rename it to match the corresponding default CSV file in the `\AID_6.7\HP_Data_Analysis\Logger` subdirectory.
Logger_AID_ Schema_ SearchExport.csv	Sample file shipped with the product. Used by the Logger_AID_Schema.adv file provided. To use a sample file, copy the file and rename it to match the corresponding default CSV file in the `\AID_6.7\HP_Data_Analysis\Logger` subdirectory. Later, when you generate real CSV data files, you can save them with different

File	Description
	names. ADV projects allow you to select different CSV data source files and then you can save your projects with different names for different CSV files.
Logger_Fieldset_ _AID_ Schema.xml.gz	Import this fieldset into Logger. You can use them to run a search for the AID_ Schema data sets and export those event fields to a .csv for use by the provided ArcSight Interactive Discovery projects. If upgrading from prior release, delete the current field set **before** importing the new .gz file.
Logger_Report_ AID_Schema.cab	You deploy the report bundle to the Logger machine. The CAB file contains an AID_Schema report required to output data for consumption by Interactive Discovery. If upgrading from prior release, delete the current report **before** importing the new .gz file.
PriorityByBin.asl	Enables color sorting by ArcSight ESM Active Channel Priority.

System Requirements

Interactive Discovery can only be installed on Windows operating systems. For system requirements recommended for optimum performance, see the *Advizor Implementation Guide* included in the ZIP file download.

ESM Recommendations: In addition, these recommendations are made for best performance for ESM. These recommendations do not apply to Logger.

- 16 GB heap size
- Reports archived in separate process.

16 GB Heap Size

For high performance systems, 16 GB heap size is recommended. To change the heap size:

1. Stop ESM Manager.
2. Update the file `server.wrapper.conf` with these lines:
   ```
   wrapper.java.initmemory=16384
   wrapper.java.maxmemory=16384
   ```
3. Stop and then start the manager for the changes to take effect.

AID Reports Separate Process

For best performance, configure the AID reports to be archived in their own separate process. This will help avoid memory contention with other manager resources.

To set up a separate process for reports, you must configure the `server.properties` file, and then configure each report.

1. On the Manager host, update the file `<ARCSIGHT_HOME>/config/server.properties` with this line:

   ```
   report.canarchivereportinseparateprocess=true
   ```

2. Restart the manager.

Separately, when configuring the reports, a new report parameter is made available in the Console.

1. In the Console, open the reports you are scheduling to run.
2. Right click **Edit Report**.
3. Select the **Parameters** tab.
4. Set **Generate Report in Separate Process** to true.
5. Click **Apply** to save changes.

Installing Interactive Discovery

Log in to the Interactive Discovery target system with Administrator privileges; the installer makes modifications to the registry.

1. Verify system requirements as found in the *ADVIZOR Implementation Guide*, located in the ZIP file download in `AID_6.7\Advizor.`
2. **Important:** Uninstall any previous version of ArcSight Interactive Discovery.
3. From the HPE Software Support site (https://softwaresupport.hpe.com) download the Interactive Discovery ZIP file (`AID_6.7.2.zip`) using the log-in credentials you received when you purchased ArcSight Interactive Discovery.
4. Extract the ZIP file.

   Note: By default, extract to C:\ to match default locations used in the .adv files and guide examples. If you do not extract the .zip to the c:\AID_6.7 directory the default content will have to be modified to point to the new directory structure that you have chosen. This is done in the project by using the "Manage Data Sources" under the File Menu Option.

5. Browse to `AID_6.7\Advizor`. Depending on your system, launch either the 32-bit or 64-bit version of `ArcSight Interactive Discovery Bundle.exe.`

   Note: The *ADVIZOR Implementation Guide* recommends 64 bit.

6. Follow the instructions in the installation wizard to set up Interactive Discovery.
7. When the installation is complete, review the "What's New" section of the online help for important information regarding this release.

Uninstalling Interactive Discovery

To uninstall Interactive Discovery:

1. In Windows, launch Control Panel.
2. Follow the steps for your version of Windows to uninstall the application.
3. Delete the directories under c:\AID_6.7\Content (this is the default content). Do not delete the c:\AID_6.7 directory as this is where your own personal projects and data have been saved.

To uninstall the AID content from the ESM Manager:

1. Launch ArcSight Console.
2. In the Navigator panel, click the **Packages** tab.
3. Open the **ArcSight Interactive Discovery** group.
4. Right-click the **ArcSight Interactive Discovery** package and choose **Uninstall Package**.
5. Right-Click the **ArcSight Interactive Discovery** package and choose **Delete Package** (required or ESM may incorrectly assume the package is already there and not install the CURRENT content that has been released).

To uninstall the AID fieldset content from Logger:

1. Launch Logger.
2. In the Search box, type *fieldsets*.
3. In the search results, locate the AID fieldset content to be deleted.
4. Click the X on the right side of the entry to delete the content.

To uninstall the AID report content from Logger:

1. Launch Logger.
2. Click Reports from the main menu.
3. Select Category Explorer.
4. Right click on ArcSight Interactive Discovery and select **Delete**.
5. Click **Yes** to confirm deletion.

Extracting the Other Zip Contents

When you unzip `AID_6.7.2.zip`, it creates the following folder structure:

- `AID_6.7\Advizor (32-bit and 64-bit directories)`
- `AID_6.7\Content\ESM`
- `AID_6.7\Content\Logger`
- `AID_6.7\HP_Data_Analysis\ESM(and \Logger)`

When you extract the content files, the `AID_6.7.2.zip` file creates and writes the files to an `AID` subdirectory.

> **Note**: By default, extract to C:\AID_6.7 to match default locations used in the .adv files and guide examples.

Verify that all the files in the ZIP file were extracted.

After extracting the files, you can move and copy them using these guidelines:

- You can copy and rename ADV project files and put them wherever you want.
- You can copy and rename CSV files as necessary, provided there is a corresponding INI file with the same name in the same folder.
- The "CONTENT" directory holds all the project and sample files. It is recommend that you do not modify these sample files. Copy the `AID_6.7\Content\ESM and AID_6.7\Content\Logger` files to the system where your ArcSight Console is installed.
- **Important:** The "HP_Data_Analysis" directory is the working directory where you save your event files for analysis and visualization.
- You can change the source file that a project uses and then save the project with a different name. Source files are always CSV files.

Chapter 3: Generating ESM Data

ArcSight Interactive Discovery operates on data exported from your daily event flow from ArcSight **focused reports** and **active channel**, that filter and aggregate events into a schema that is ready to consume by Interactive Discovery. This chapter describes the process of loading data from ESM into Interactive Discovery.

Interactive Discovery ships with a sample data set loaded into its default CSV files. You can use this data set as a tutorial for getting familiar with the ArcSight Interactive Discovery projects and tools, as outlined in chapters 4 and 5.

- "ESM Focused Reports " on the next page
- "ESM Active Channel " on page 20

Importing the Interactive Discovery Package into ESM

Use the ArcSight Console import capability to import the `ArcSight Interactive Discovery.arb` content file found in `C:\AID_6.7\Content\ESM`, as described below.

1. Save the `ArcSight_Interactive_Discovery.arb` content file to a network location accessible to your ArcSight Console.
2. Launch ArcSight Console.
3. In the Navigator panel, click the **Packages** tab.
4. Click **Import**, at the top of the Packages tab.
5. Access the ARB file and click the **Open** button.
6. On the **Packages for Installation** dialog, click **Next**.
7. ArcSight Console creates an ArcSight Interactive Discovery folder.

To verify that installation was successful and the content is accessible in ESM:

1. In the Navigator panel, go to **Filters** and navigate to the ArcSight Interactive Discovery Filters folder. Verify that the folder appears as shown below.

2. In the Navigator panel, go to Reports and navigate to All Reports. Verify that the the ArcSight Interactive Discovery folder appears as shown below.

3. If you do not see these filters and reports, right-click in the Navigator panel and select Refresh.

> **Note:** The reports shown above are focused reports. There is also a subfolder called Templates containing AID_Schema base reports from which you can create other focused reports.

See "Generating ESM Data" on the previous page.

ESM Focused Reports

For ESM, Interactive Discovery includes the report templates listed in the following table. When combined with the filters listed in the Filter table, they make ESM focused reports, which are listed in the Focused Report table. Once installed, find these reports in the ArcSight Console Navigator's **Reports** resource:
`/All Reports/ArcSight Interactive Discovery/Templates/`.

Template	Description
AID_ Schema	This report shows a selection of event fields useful for analyzing security data. It makes working in the Explorer easier and consumes less space when transporting the data from the ESM Manager to the Explorer.

The following filters are used by the Interactive Discovery focused reports to filter for the specific types of events that you are interested in for your analysis. These filters are located in the ArcSight Console Navigator's **Filters** resource: `/All Filters/ArcSight Interactive Discovery`.

Filter	Description
Attacks	Exports traffic that resembles attacks.
Attacks Targeting Critical Servers	Exports traffic that indicates potential attacks against servers classified as Very High criticality in `/All Asset Categories/ System Asset Categories/Criticality/Very High`.
Authentication and	Shows authentication and authorization events (logins, password changes, and so on).

Filter	Description
Authorization	
Intrusion Detection Systems	Exports just intrusion detection system events.
Firewall Events	Shows only firewall events.
Operating System	Selects all operating system events (such as logon/off, resource failures, system reboot).

These reports and filters are combined as focused reports, which are located in the ArcSight Console Navigator's **Reports** resource: `/All Reports/ArcSight Interactive Discovery…`. All the Interactive Discovery reports filter out ESM internal events (self-auditing events).

Focused Report	Description
All - AID_Schema	Compiles all events (no filters applied) in the past 2 (by default) hours using the AID_Schema of data.
Attacks - AID_Schema	Compiles all events that involve attacks in the past 2 (by default) hours using the AID_Schema of data.
Attacks Targeting Critical Servers - AID_Schema	Compiles all events that targeted critical servers in the past 2 (by default) hours using the AID_Schema.
Authentication and Authorization - AID_Schema	Compiles all events classified as authentication and authorization events in the past 2 (by default) hours using the AID_Schema of data.
Firewall Events - AID_Schema	Compiles all firewall events in the past 2 (by default) hours using the AID_Schema of data.
IDS - AID_Schema	Compiles all IDS events in the past 2 (by default) hours using the AID_Schema of data.
Operating System - AID_Schema	Compiles all operating system events (such as resource failures and system reboot) in the past 2 (by default) hours using the AID_Schema of data.

Reports Data from ESM

Generating data for an Interactive Discovery project is a multi-step process. These steps are outlined below and detailed in the pages to follow.

1. Import the ESM Content files. See "Importing the Interactive Discovery Package into ESM" on page 15.
2. From the ArcSight Console, run one of the Interactive Discovery focused reports. You can run them as needed or schedule them to run regularly.
3. Open the report output file and save it to `C:\AID_6.7\HP_Data_Analysis\ESM\ AID_Schema.csv`.

   You can specify any file name.

   In addition, you must save an INI file with the same name as the CSV file. You can copy and rename the CSV files that come with the ESM Content `in AID_6.7.2.zip`.
4. If you have a separate Interactive Discovery system, copy the resulting CSV file there. The CSV and its matching INI file can go in any folder.
5. Open the Interactive Discovery ADV project file (ArcSight_AID_Schema.adv). When you open the Interactive Discovery project you can point it to the appropriate data source. To change or add data source files in Interactive Discovery, select **File > Manage Data Sources**..

To incorporate Interactive Discovery into your everyday operations, schedule one or more of the Interactive Discovery focused reports to run once at a set time every day, and use their output to analyze and build reports about the day's network security events. For instructions about how to schedule reports, see the Console online help topic "Scheduling Tasks."

Tip: Avoid scheduling more than one Interactive Discovery report to run at the same time. Scheduling them to run at different times gives the file output names unique date/time stamps.

Running an ESM Focused Report

1. In the Navigator panel Reports resource tree, go to /All Reports/ArcSight Interactive Discovery.
2. Right-click the focused report you wish to run and select **Run > Report with defaults**.
3. The report will likely take several minutes to run, depending on how much data it has to process. As the report runs, the message
   `[date, time] Creating report…Please wait…`
   is displayed in the Messages bar at the bottom of the Console. When the report is finished running, the message
   `[date, time] Launching report in the browser window…`
   is displayed. Both of these processes may take several minutes. When the report is finished running, it opens in a browser window with numbered lines in a grid format.

The report defaults are set to 100,000 lines of output and 2 hours. To increase these values, edit the report (right-click the report's icon and choose **Edit Report**) and change the values as required.

NOTE: ArcSight has tested the reports to 100,000 and found acceptable performance. Increasing the report parameters may require increasing ESM memory management parameters.

See "Save ESM Report Data to Interactive Discovery" on the next page

Building a Focused Report

In ESM, you can use one of the existing ArcSight Interactive Discovery template reports for building a new focused report with your own specifications. The only report changes we encourage are changes in the filter conditions to select a specific set of events to be exported into Interactive Discovery.

To create a new focused report:

1. In the Navigator panel Reports resource tree, click on the **Reports** tab and go to `/All Reports/ArcSight Interactive Discovery/Templates`....
2. Right-click AID_Schema report and select **New Focused Report**.
3. In the Focused Report Editor in the Inspect/Edit panel, select the **Attributes** tab and name the report in a way that distinguishes it from its original.
4. Click the **Parameters** tab and change any of the values as appropriate. These values are the same ones you set when running a new or archived Report.
5. Click **Apply** to make changes and keep the editor open.
6. Click **OK** to store the definition in the resource tree in the same folder as the original report and close the editor.

Scheduling a Focused Report

You can schedule a focused report. Once the report has run, save it as AID_Schema.csv, and copy it to the Interactive Discovery system, as described in"Save ESM Report Data to Interactive Discovery" on the next page.

1. In the **Reports** resource tree, select the **Report Definitions** tab.
2. On the **Reports** tab, right-click the report you wish to schedule and select **Schedule for archiving | Report**.
3. On the **Jobs** tab, click the **Add** button.
4. Enter a name under the **Jobs** field and a description for the report under the **Description** field.

   If the reports you generate for a full day's events contain more than 100,000 lines, you should modify the report to run in a shorter time frame, then schedule the report to run at those time intervals throughout the day.

For example, if you set the report to run 6 hours worth of data, schedule the report to run at 6-hour intervals, such as 12:00 a.m., 6:00 a.m., 12:00 p.m., and 6:00 p.m.

5. Select **Click here to set up schedule frequency**.
6. In the **Job Frequency** dialog, select your desired settings for job scheduling.
7. When the report has run, follow the instructions in Step 2: Save Report as "AID_Schema.csv" and Copy to Interactive Discovery System as described in "Save ESM Report Data to Interactive Discovery" below.

Save ESM Report Data to Interactive Discovery

1. After saving your report results as a CSV file, copy it to the Interactive Discovery system.
2. Make sure to save an INI file with the same name in the same folder. The ArcSight Interactive Discovery project requires that its data source and INI files have the same name and be in the same folder.
3. Navigate to **All Archived Reports > ArcSight Interactive Discovery** and find the report you just ran. The report is marked with the date and time of last running, and the corresponding CSV file.
4. Save the file to the local Console system.
   - If Interactive Discovery is installed on its own system, save the file to a location on the Console. By default, reports are saved to `$ARCSIGHT_HOME\current\tmp\reports`, although you can save the file to any directory.
   - If Interactive Discovery is installed on the same system as ArcSight Console, save the file to the folder where the other Inte.ractive Discovery files are located. For example: `C:\AID_6.7\HP_Data_Analysis\ESM`
5. If Interactive Discovery is installed on its own system, copy the CSV file from the Console to the Interactive Discovery system. The intent is that you place this file in the folder `C:\AID_6.7\HP_Data_Analysis\ESM`, but the only two unbreakable rules are:
   - The CSV file has to be in the same folder as the corresponding INI file (that is, with the same name prefix).
   - The appropriate Interactive Discovery project has to be looking for its data source in that folder.

ESM Active Channel

For ESM, Interactive Discovery includes the Active Channel listed in the following table.

Focused Report	Description
AID - All	Shows all events (non-arcsight internal events) in the past 2 (by default) hours using the AID_Schema of data.

Focused Report	Description
AID - Attacks	Shows all events that involve attacks in the past 2 (by default) hours using the AID_Schema of data.
AID-Attacks Targeting Critical Servers	Shows all events that targeted critical servers in the past 2 (by default) hours using the AID_Schema.
AID - Authentication and Authorization	Shows all events classified as authentication and authorization events in the past 2 (by default) hours using the AID_Schema of data.
AID - Intrusion Detection	Showss all IDS events in the past 2 (by default) hours using the AID_ Schema of data.

Active Channel Data from ESM

Follow these steps to save the .csv file for active channel data from ESM.

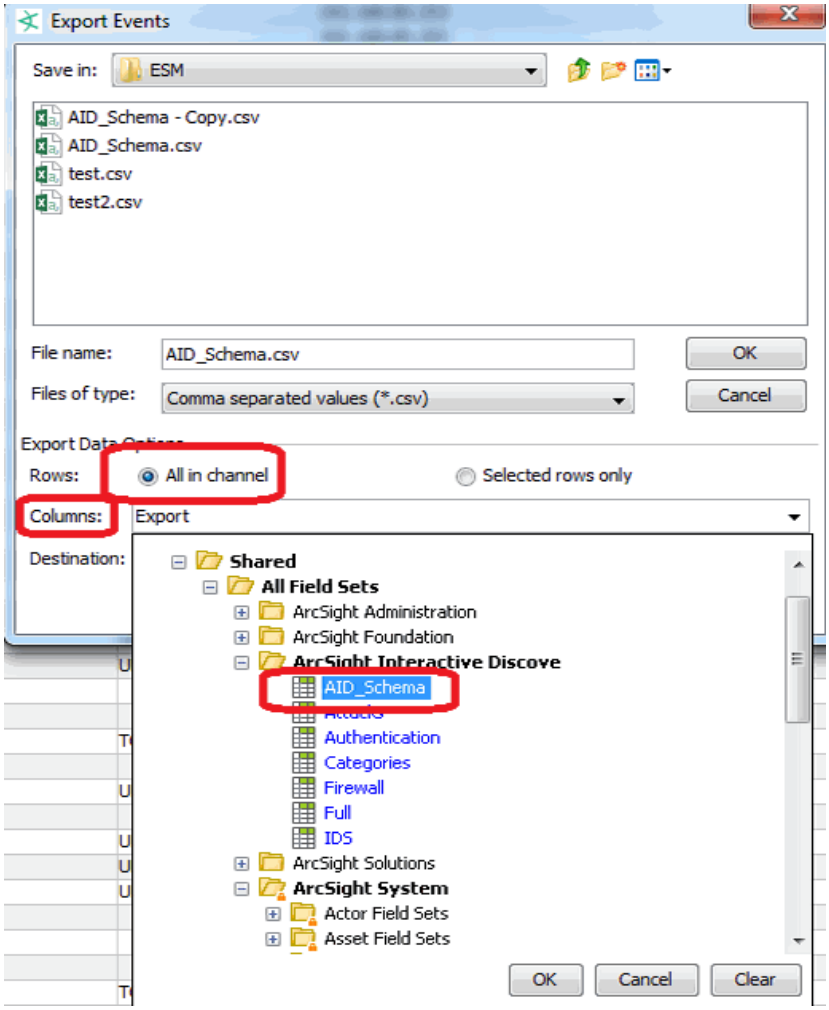
1. Import the ESM Content files. See "Importing the Interactive Discovery Package into ESM" on page 15.
2. Open the active channel that you selected (for example, AID- Firewall Events).

How to Extract ESM Active Channel Data to Interactive Discovery

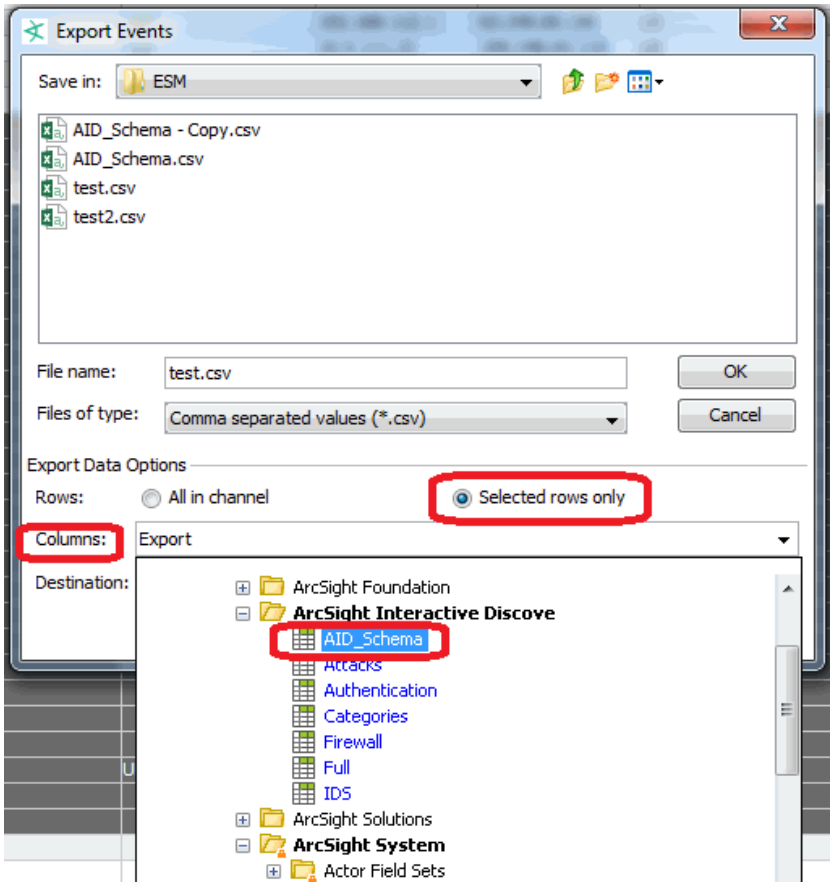
Follow these steps to extract data.

1. In the active channel, you can export selected rows or all rows in the channel.

2. For **All in the channel**, right-click when all rows are selected, then select **Export**.



3. Save the file to `C:\AID_6.7\HP_Data_Analysis\ESM`.
4. Keep the **All in channel** option active and use the **Columns** drop-down menu to select **AID_Schema** as the columns.
5. For **Selected rows only**, highlight the selected rows and right-click, then select **Export**.



6. Save the file to `C:\AID_6.7\HP_Data_Analysis\ESM.`
7. Click **Selected rows only**, and select **AID_Schema** for **Columns**.

Save ESM Active Channel Data to Interactive Discovery

1. If Interactive Discovery is installed on the same system as ArcSight Console, save the file to the folder where the other Interactive Discovery files are located. For example: `C:\AID_6.7\HP_Data_Analysis\ESM`
2. If Interactive Discovery is installed on its own system, copy the CSV file from the Console to the Interactive Discovery system. The intent is that you place this file in the folder `C:\AID_6.7\HP_Data_Analysis\ESM.`

Chapter 4: Generating Logger Data

This chapter describes the process of generating data in Logger using a search or running a report and sending it to Interactive Discovery.

Interactive Discovery ships with a sample data set loaded into its default CSV files. You can use this data set as a tutorial for getting familiar with the ArcSight Interactive Discovery projects and tools.

This section includes the following topics

Overview: Logger Data

In Logger, there are two ways to generate data for Interactive Discovery: You can do a search using the fieldsets provided or you can the report provided. The steps for each method are outlined below and detailed in the pages to follow.

1. Generate data from a Logger search.
   a. Import the Logger fieldset files.
   b. Start a search and enter the search criteria.
   c. Select one of the imported fieldsets.
   d. Export the search to a CSV file.
2. Generate data from Logger reports.
   a. Import the Logger report and the related queries provided in the CAB file.
   b. Run the imported report.
   c. Export the report results to a CSV file.
3. If you have a separate Interactive Discovery system, copy the resulting CSV file there. The CSV and its matching INI file can go in any folder.
4. Open the Interactive Discovery ADV project file (ArcSight_AID_Schema.adv). When you open the Interactive Discovery project you can point it to the appropriate data source. To change or add data source files in Interactive Discovery, select **File > Manage Data Sources**.

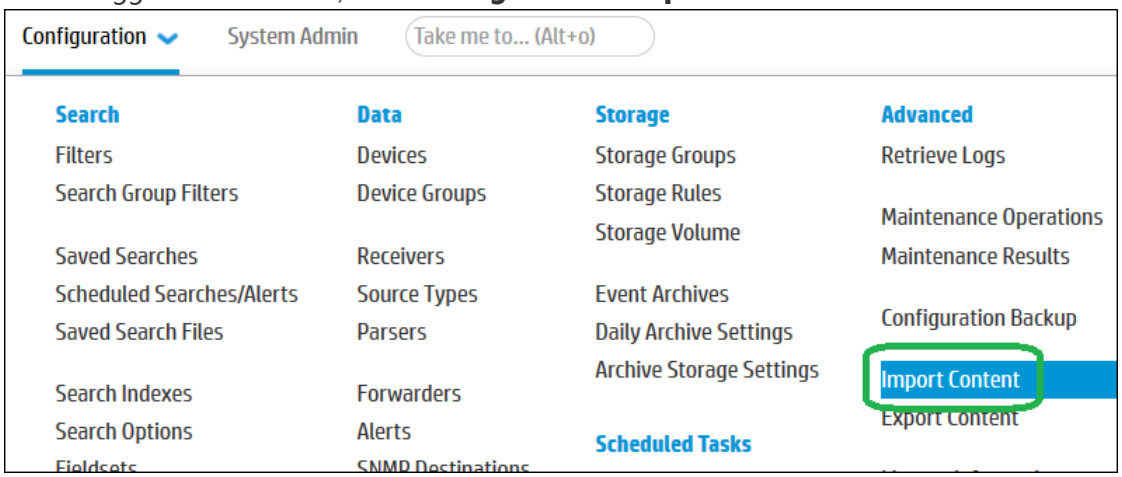
Using the Logger Search Method

In this procedure you import the provided Logger fieldsets, run searches that use them, and export the result as a CSV file. Then you save the CSV file as the data source for your Interactive Discovery project.

Importing the Interactive Discovery Package into Logger

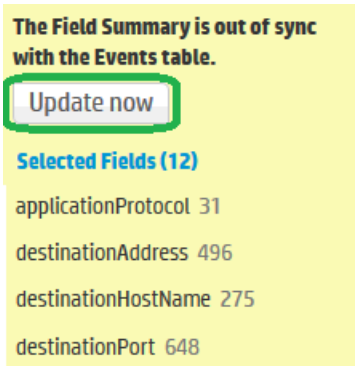
The Logger content consists of a fieldset and a report. The first step is to import the fieldset content, and then deploy the report content. Use the Logger import capability to import the Logger fieldsets, as described below.

1. Save the logger fieldset file to a network location accessible to Logger.
2. Launch Logger.
3. In the Logger user interface, select **Configuration > Import Content**.



4. On the **Import Content** dialog, click **Browse**.
5. Browse to the fieldset to import and click **Open**.
6. On the **Import Content** dialog, click **Import**.

   The fieldset file you imported is displayed.
7. To verify that the selected field sets was properly imported, click **Configuration > Fieldsets** and verify that the fieldset you imported is displayed in the list.
8. Select the imported fieldset from the list.
9. To complete the update to the new field set, click **Update now** in the summary section in the lower-left of the Logger window. This enables the field summary list to reflect the fields available in the selected field set.



10. A summary of the deploy results is displayed
11. Select **Reports > Report Explorer** to verify the report category and report were imported and then run the reports to verify that they run correctly.
12. See "Generating Logger Data" on page 24.

Logger Fieldsets

For Logger, Interactive Discovery includes the following fieldsets. Once installed, find these fieldsets in the Logger UI by clicking **Configuration > Fieldsets**.

Fieldset	Description
AID_ Schema	This fieldset shows a selection of event fields useful for analyzing security data. It makes working in the Explorer easier and consumes less space.

Run a Logger Search

In this procedure, you export the results of a Logger search as a CSV file, then open the CSV file in AID. Refer to the *Administrator's Guide* for ArcSight Logger for details on how to export a search. The general procedure is as follows:

1. In the Logger user interface, select **Analyze > Search**.
   - Enter any search criteria whose results you want to analyze with Interactive Discovery and click **Go**.
2. Select one of the AID fieldsets from the **Fieldset** dropdown box. By default, *All Fields* is selected.
3. Click the Export down arrow to export the results to a file. Set these options:
   a. Select **Save to local disk**.
   b. Use the default format of **CSV**.
   c. Do not check **All Fields**. It will use the fields in the fieldset.
4. Click **Export**.
5. Right-click on **Download results** to specify where to save the CSV file.

To use the AID project included in the download (`Logger_AID_Schema.adv`), specify the CSV file name associated with that project.

If you want to build another AID project, specify a file name to help you identify it, and then create another AID project to use that file.

6. Click **Done**.
7. If Interactive Discovery is installed on its own system, copy the CSV file from the Logger system to the Interactive Discovery system. The intent is that you place this file in the folder `C:\AID_6.7\HP_Data_Analysis\Logger`, but the only two unbreakable rules are:
   - The CSV file has to be in the same folder as the appropriate AID_Schema INI file with the same name prefix.
   - The appropriate AID_Schema Interactive Discovery project has to be looking for its data source in that folder.

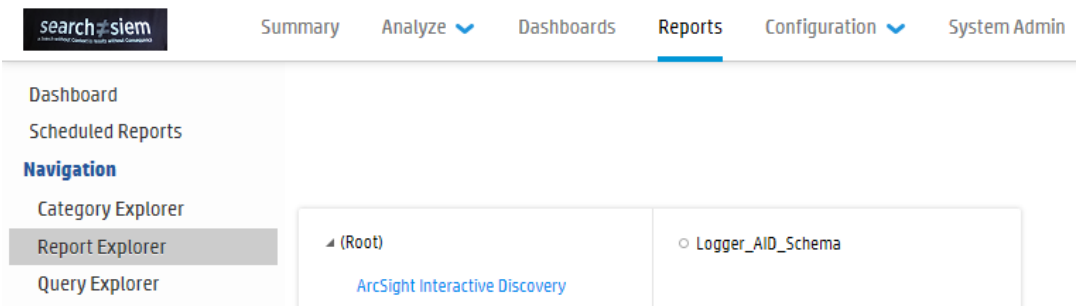
Using the Logger Report Method

The Logger reports and their associated queries are bundled in CAB files. In this procedure you deploy each report bundle, run the report and export the result as a CSV file. Then you use the CSV file as the data source for your Interactive Discovery project.

Import Logger Reports

Import the reports, bundled as a CAB file, as described below.

1. Select **Reports > Deploy Report Bundle**, under the Administration section.
2. On the **Deploy Repository Bundle** dialog, click **Browse** and select (open) the CAB file to be imported and click **Upload**.
3. On the **Deploy Repository Bundle** dialog, click **Deploy**. 6. A summary of the deployment results is displayed.
4. Go to **Reports > Report Explorer** to verify the report category and report were imported:



The report category is "ArcSight Interactive Discovery."

Running the Logger Report

Use the following general procedure to run one of the Logger reports and save the results as a CSV file. For details refer to the Logger Administrator's Guide for your version of Logger.

1. Select **Reports > Report Explorer > ArcSight Interactive Discovery**.
2. Select a report to run.
3. Click the **Run Report** option.
4. Click on the filter tab, if you want to limit the data to events where certain fields contain certain values.
5. Click the **Run** button.
6. In the report parameters window you can select the start time. For example **$Now - 1d** for events from the last two days until now.
7. Click **Run Now**.
8. When the report completes, select **Save File**. Logger saves the file as a CSV file.
9. If Interactive Discovery is installed on its own system, copy the CSV file from the Logger system to the Interactive Discovery system. The intent is that you place this file in the folder `C:\AID_6.7\HP_Data_Analysis\Logger`, but the only two unbreakable rules are:
   - The CSV file has to be in the same folder as INI file with the same name prefix.
   - The appropriate Interactive Discovery project has to be looking for its data source in that folder.

Chapter 5: Open Project in Interactive Discovery

Interactive Discovery ships with these projects:

- ArcSight_AID_Schema.adv
- Logger_AID_Schema.adv

ESM and Logger use different sets of fields. Each AID project makes use of product-specific data.

Which project file you open depends on what data you generated and from where.

1. On the Interactive Discovery system, launch Interactive Discovery. You can launch it by double-clicking the ADV file. You can also select **Open Project** at the **Getting Started** screen and select the appropriate project file.
2. Each ADV file remembers the absolute path to its associated data source file. When you first open a project you might get a **Locate Missing Data File** dialog that reports the path of the file it cannot find.

   Use the browse button to navigate to the folder where the data source file is located and click **OK**. (Make sure the INI file of the same name is present.)

   If you had to browse to the file, select **File > Save Project** to preserve this location.

   Interactive Discovery allows you to use a CSV file as a data source. A matching INI file in the same folder is required.

Chapter 6: Navigation Overview

Each Interactive Discovery project contains a set of tabs that enable you to analyze your network security data using different interactive graphics.

Follow the instructions in "Open Project in Interactive Discovery" on page 29 to open a project. When the project view opens, the window displays the Overview tab:

To familiarize yourself with Interactive Discovery's toolbars, click the Help icon (a red question mark) and browse the topic "Interactive Discovery Toolbars."

You can toggle the toolbar for each individual chart or list panel by clicking the small triangle in the gray bar beneath the panel, as shown below.

Click the arrows at the right end of the tab bar to scroll it left and right.

In most charts you can hover the cursor over a data point, (bar or pie slice, for example) to see details of the data point.

The chart colors are from the event's priority as determined by the threat priority formula. To change the color, use the **Color by** pull-down menu in the toolbar. For information on event priorities, see the section in *ESM 101* entitled, “Life Cycle of an Event through ESM."

To see the details of a chart element (bar, pie wedge, and so on), hover over it. You can also click on an element to filter the view in all tabs. Right-click and select **Select All** to restore the views. Use the online help for complete information on chart navigation.

Note: that the sample data provided contains events where some of the values are NULL. In some cases, values may have been removed for publication. Your results will be different.

Chapter 7: Interactive Discovery AID_Schema Project

The tabs provide multiple unique views of the data contained in this data set. Use the reports provided in the package (the ARB file) to generate the data appropriate for the project.

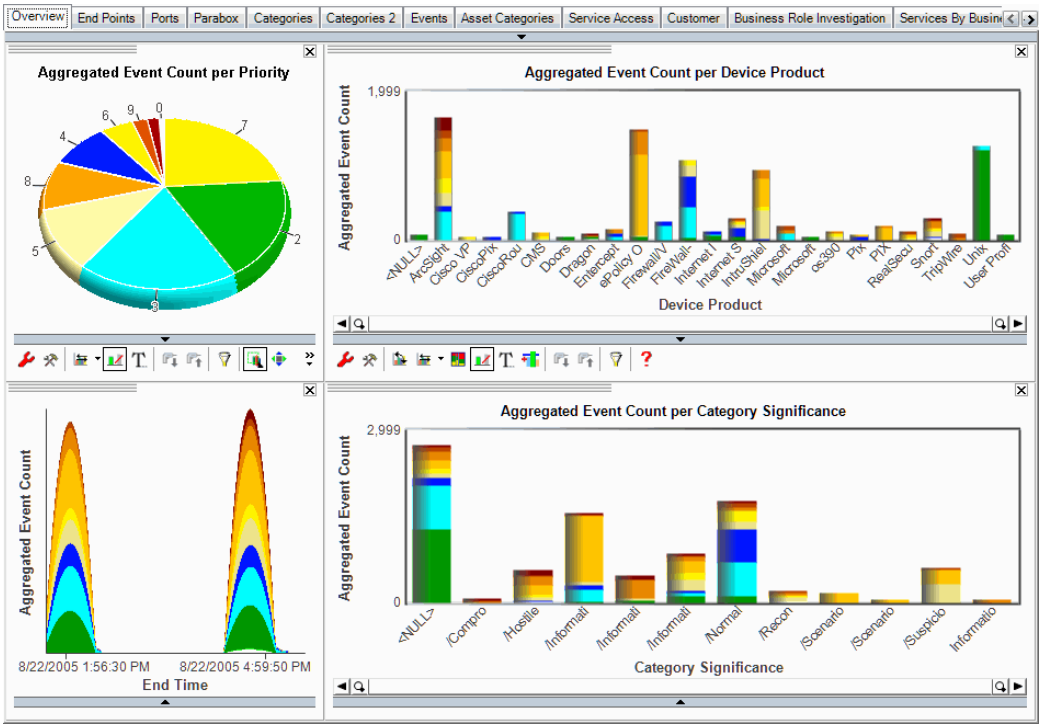
The AID schema contains event fields that ArcSight considers the most common event criteria to evaluate for most security situations and reduces the data to be processed.

> The examples and visualizations here make use of data from the ESM project. Examples and visualizations from Logger data will be slightly different from what is shown here.

Overview Tab

In the ArcSight Advizor Application the Overview tab contains four charts.

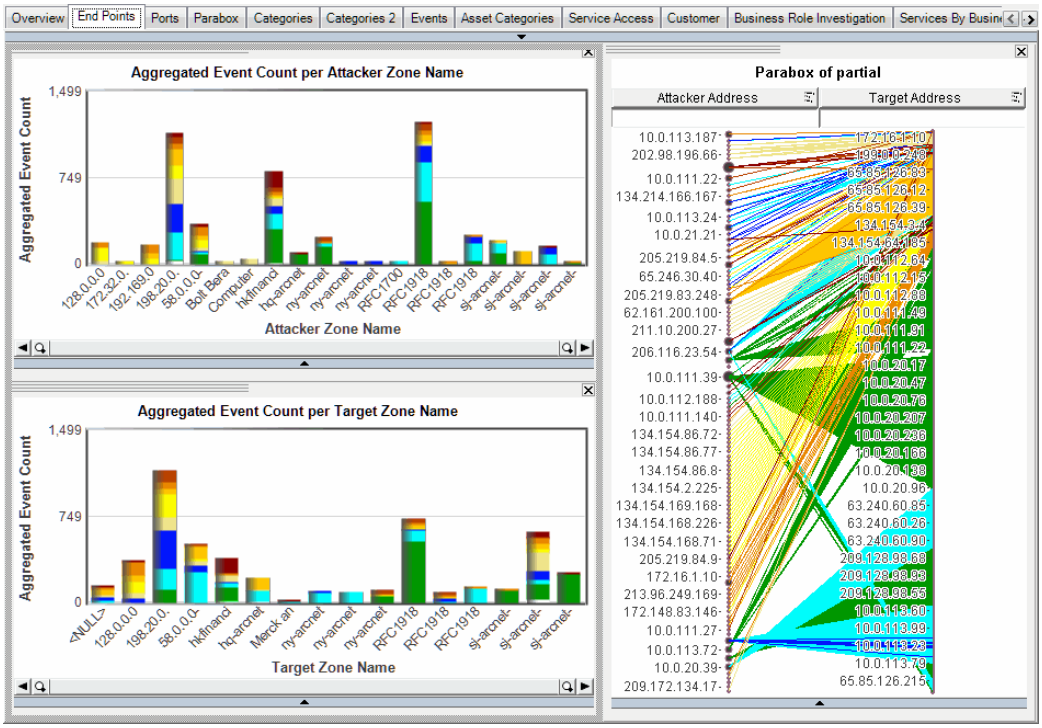
- **Aggregated Event Count per Priority**: shows a pie chart of the number of events of each priority as determined by the ArcSight priority formula.
- **Aggregated Event Count per Device Product**: shows the number of aggregated events by device product (ArcSight, MS Windows, Unix, and so on).
- **Aggregated Event Count by Time**: shows the times when events occurred.
- **Aggregated Event Count per Category Significance**: Shows the number for each category of significance (hostile, normal, warning, and so on).



End Points Tab

The End Points tab contains three charts:

- **Aggregated Event Count per Attacker Zone Name:** Shows number of aggregated events that occurred in various attacker IP address zones. You can use the right-click menu to drill down to individual IP addresses.
- **Aggregated Event Count per Target Zone Name:** Shows number of aggregated events that occurred in various target IP address zones. You can also right-click the menu to drill down to individual IP addresses.
- **Attacker/Target Address parabox:** The parabox shows connections from the attacker to the target. Select one of the bars in a bar chart on the left, and the parabox displays the connections involved with those events only. Bubble size indicates the amount of activity.



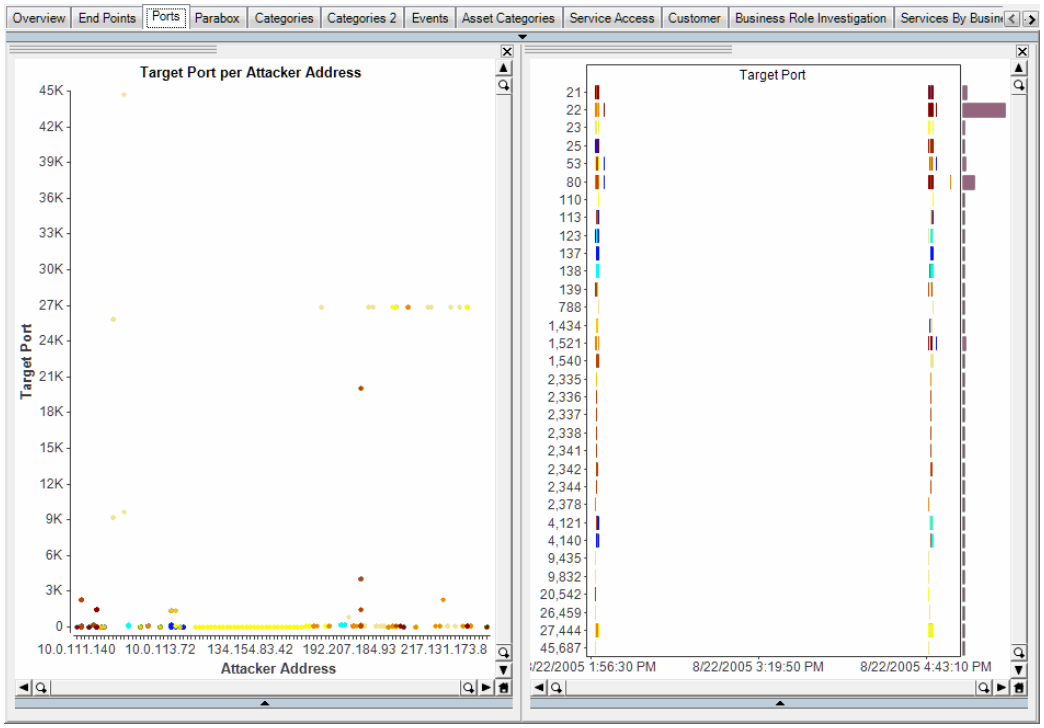
Ports Tab

The Ports tab contains two charts:

- **Target Ports per Attacker Address:** This scatter plot chart shows target ports on the left, attacker addresses on the bottom. In this chart, you can look for conditions such as services running on ports above 1024, which could warrant investigation, or you can exclude them from the view if they are not significant. Multiple systems connecting to the same port appear as a horizontal line. Vertical lines indicate one system connecting to multiple ports, which could indicate a port scan.

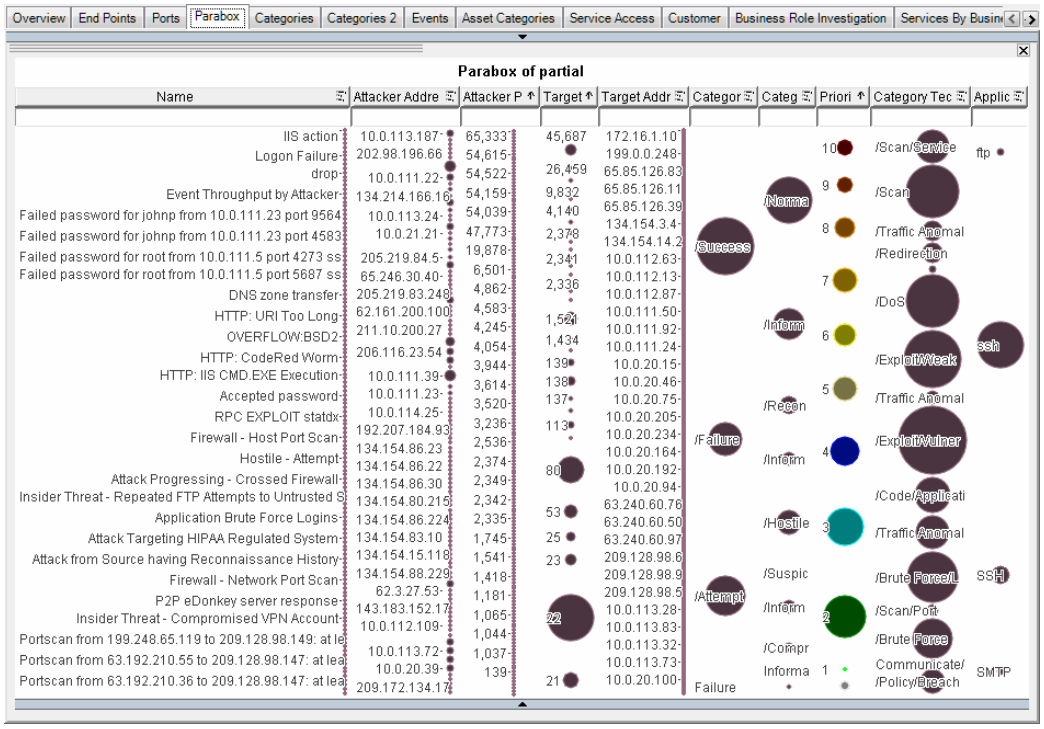
- **Target Port:** The right-hand scatter plot shows target ports on the y axis, time on the x axis. Over time, you can recognize how users access services. You might see patterns where there are lines, then a gap; something happened where no one was accessing port 80. That gap also is displayed in the Overview page histogram. You can drill down here to see details.

Use the zoom tools at the corners to magnify elements in the view.



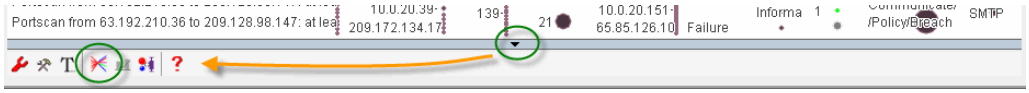
Parabox Tab

The Parabox tab contains one large view that shows the various elements of an event as bubbles of different sizes and colors. The size of the bubbles indicates the distribution of events: the larger the bubble, the more activity is indicated.

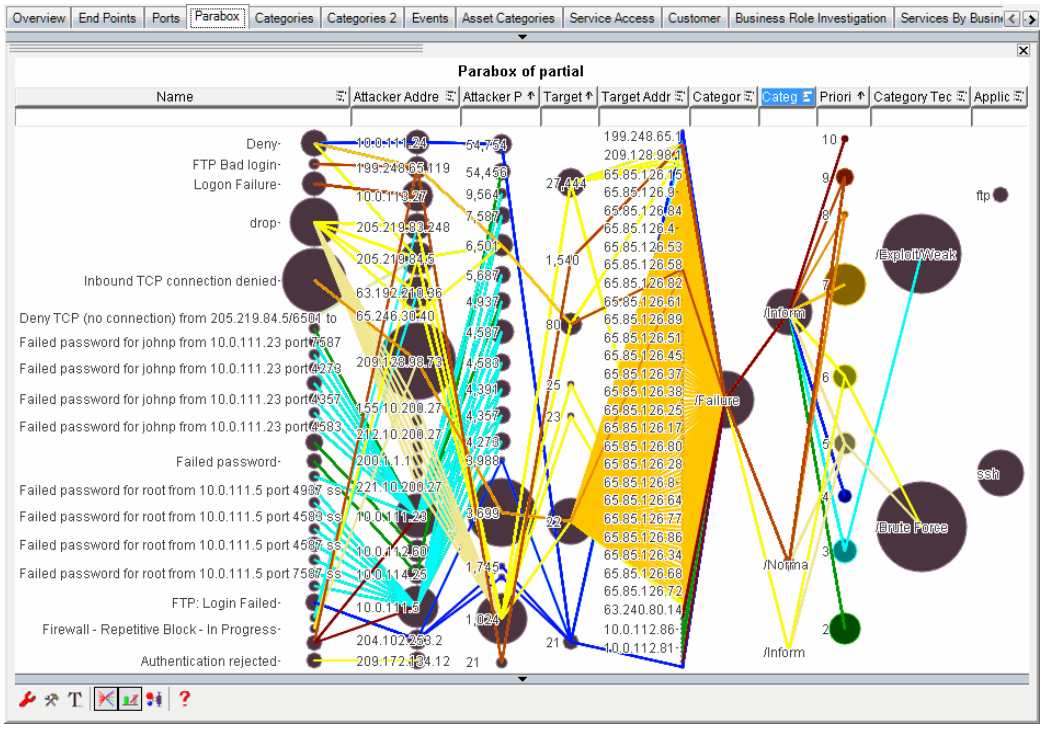


To investigate in the parabox:

1. Expand the pull-down menu at the bottom of the page to reveal data configuration tools.
2. Click on one node, such as Failure. All nodes involved with the failures remain selected.
3. Right-click in the parabox and select **Exclude Unselected** to remove unselected items.
4. Click the small gray arrow at the bottom of the display to toggle the toolbar on. Then, click the **Display axis of individual data cases** button ( )to show the connections between the nodes.



This shows that port 22 is involved with most of the failures and it goes to similar target addresses:



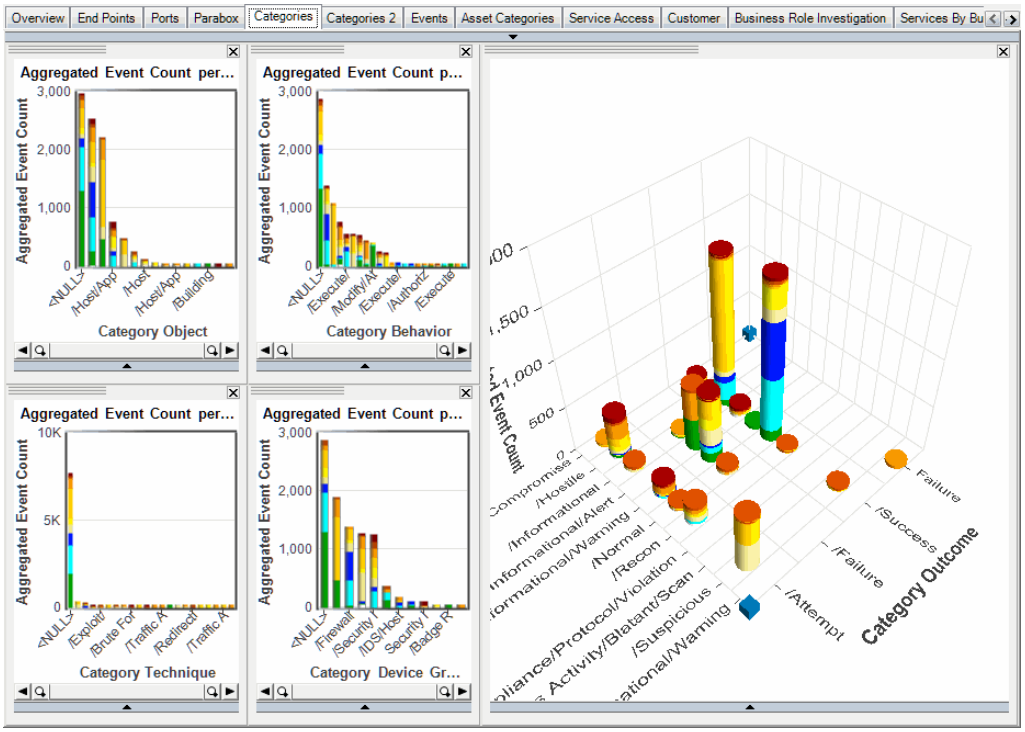
Categories Tab

The Categories tab gives you an idea of what's happening according to the ArcSight event categories. To see the details of each category, hover over the bars. You can also use the individual bars on this tab as a way to filter the rest of the views.

The Categories tab contains five charts.

- **Aggregated Event Count per Category Object**: For each category of objects (host, application, service, and so on), it shows the number of aggregated events.
- **Aggregated Event Count per Category Behavior:** For each category of behaviors (access, add, delete, execute, and so on), it shows the number of aggregated events.
- **Aggregated Event Count per Category Technique:** For each category of techniques (brute force, scan, redirection, and so on), it shows the number of aggregated events.
- **Aggregated Event Count per Category Device Group**: For each category of device groups (antivirus, firewall, operating system, and so on), it shows the number of aggregated events.
- **Aggregated Event Count by Category Significance and Outcome:** Shows the number of events

by both significance and outcome.



Categories 2 Tab

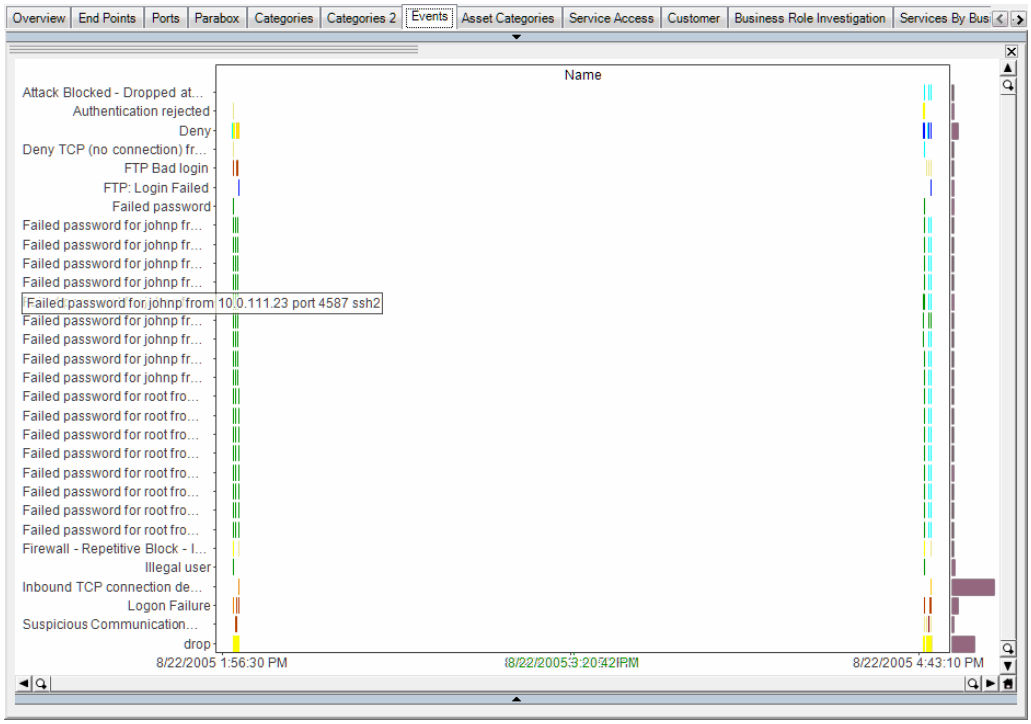
The Categories 2 tab contains two more charts:

- **Category Technique per End Time:** shows events as they occur over time by their security technique (brute force, scan, redirection, and so on).
- **Category Significance per End Time:** shows events as they occur over time, by their significance

(hostile, normal, warning, and so on).

Events Tab

The Events tab contains one large scatter plot that shows all events in the data set over time. Use the zoom tools in the corners to zoom in on patterns. Use the right-click menu to drill down to details. Use this chart to look for holes, repeated activity, lines or significant gaps. Look for dominant lines or lack of lines.

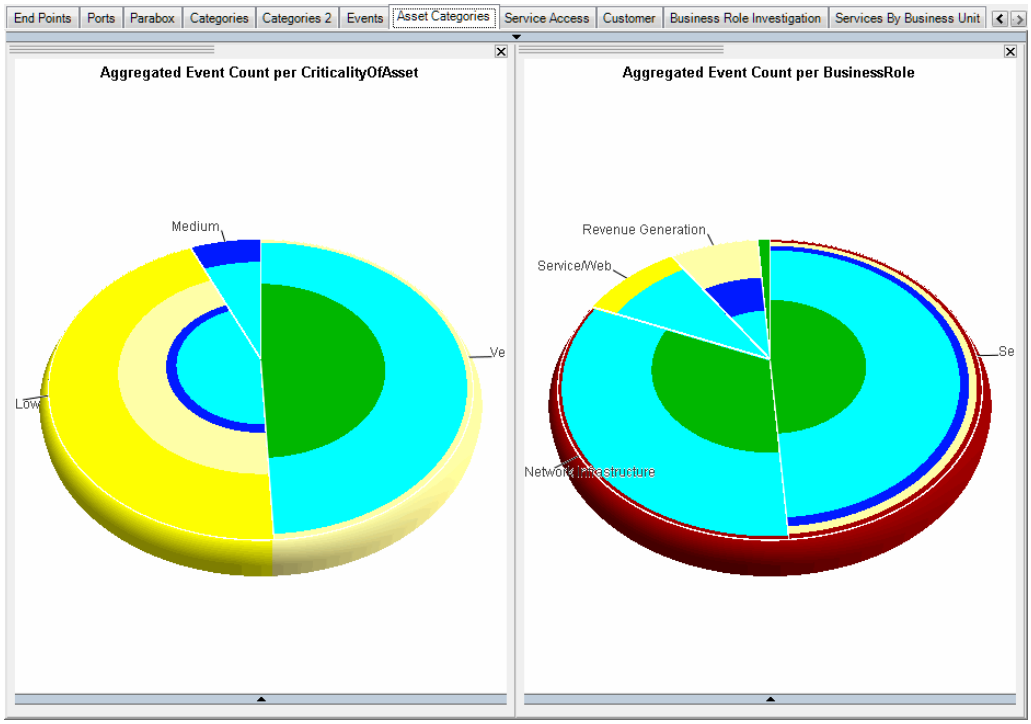


Asset Categories Tab

The Asset Categories tab shows two charts.

- **Aggregated Event Count per Criticality of Asset**: Shows the percentage of events based on the asset's criticality. Asset criticality is determined by the ArcSight priority formula.
- **Aggregated Event Count per Business Role**: Shows the percentage of events based on the asset's business role. Business role is based on the asset categories set for the assets involved in these events.

Mouse over the various sections for a description of their contents.

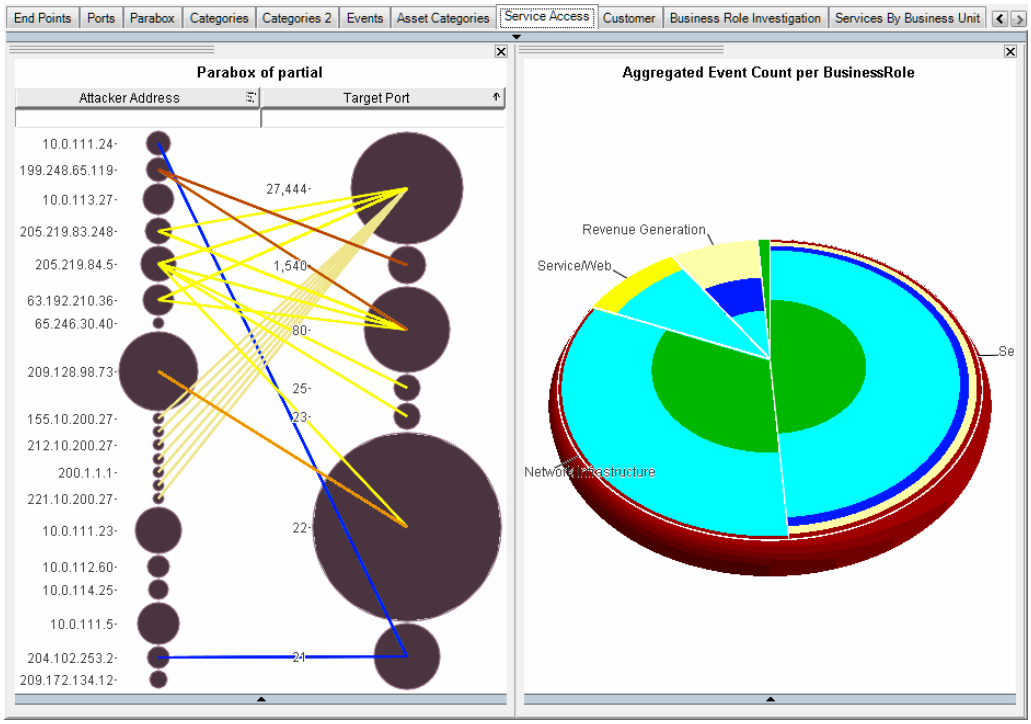


Service Access Tab

The Service Access tab contains two charts:

- **Attacker Address and Port**: This graphic shows the attacker IP addresses and their relationship with the ports involved in the subject events.
- **Aggregated Event Count per Business Role pie chart**: Shows the percentage of events based on the asset's business role. Business role is based on the asset categories set for the assets involved in

these events.



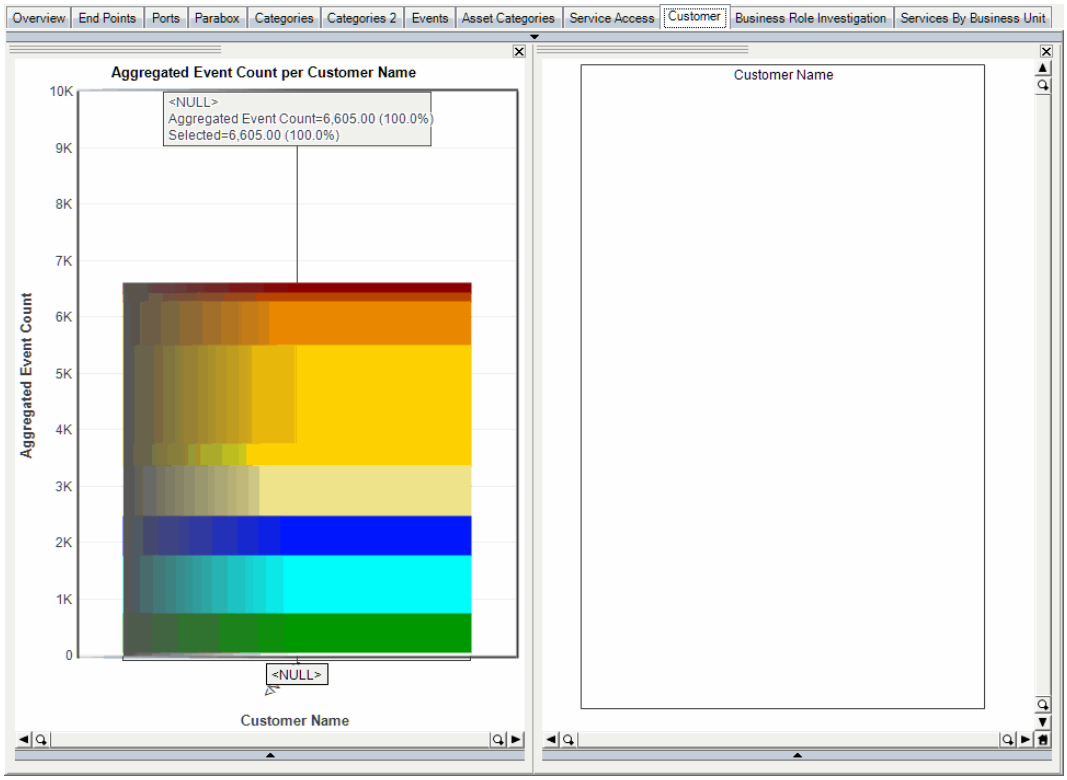
You can select target ports of interest, then see the business role of the events involved in the chart. For example, if you click the large port 22 bubble, then click the Exclude Unselected button, you see the attacker addresses and the business roles of the systems involved.

Customer Tab

The Customer tab contains two views:

- **Aggregated Event Count per Customer Name:** Shows a bar chart of all events associated with the customers configured for this system.
- **Customer Name timetable:** Shows a timetable on the right showing all customers over time when events are generated for these customers.

The example below is derived from sample data that contains no customer names. Your results may be different.



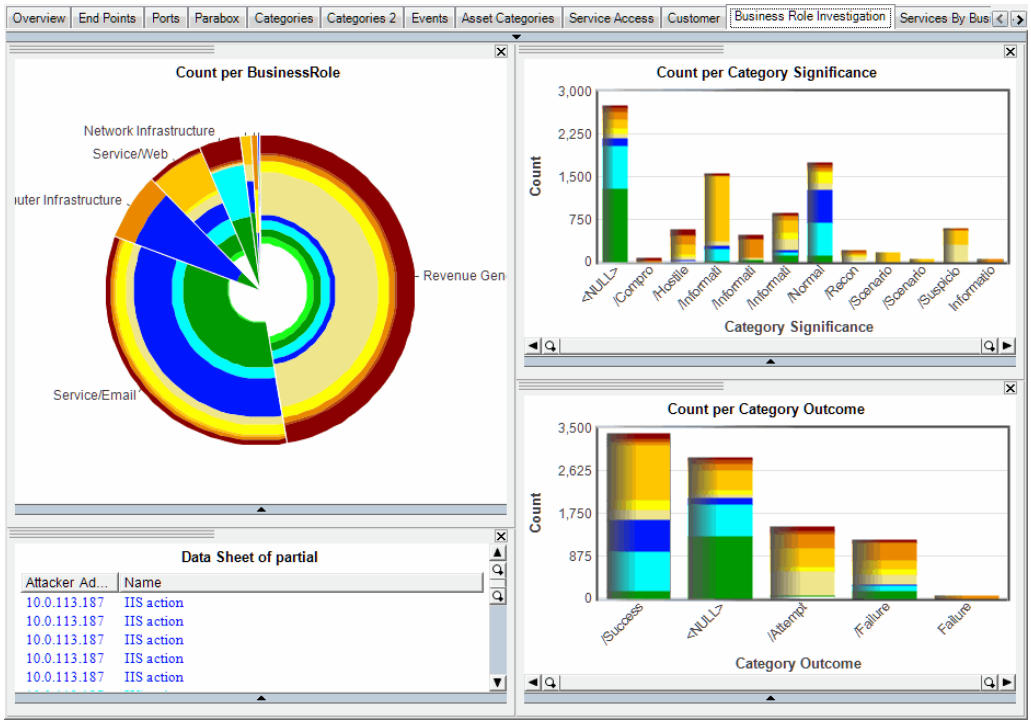
Business Role Investigation Tab

The Business Role Investigation tab contains four charts.

- **Aggregated Event Count per Business Role:** Shows the percentage of events based on the asset's business role. Business role is based on the asset categories set for the assets involved in these events.
- **Aggregated Event Count per Category Significance:** Shows aggregated events according to their significance as determined by the ArcSight event categories.
- **Attacker Address and Name List:** Shows attacker IP address and event name.
- **Aggregated Event Count per Category Outcome:** Shows aggregated events classified as successes, failures, and attempts.

Use the Business Role Investigation tab to map event outcomes to the business systems targeted. For example, you would want to see only traffic categorized as Normal occurring on revenue-generating systems. If there are any Compromise events, you can use this view to verify that they are not occurring on a revenue-generating system. If there is a compromise occurring on a revenue generating system, you can see the outcome of the event: attempt, failed, or success.

You can click the Success bar to select those events, then use the other views to see which systems were involved.

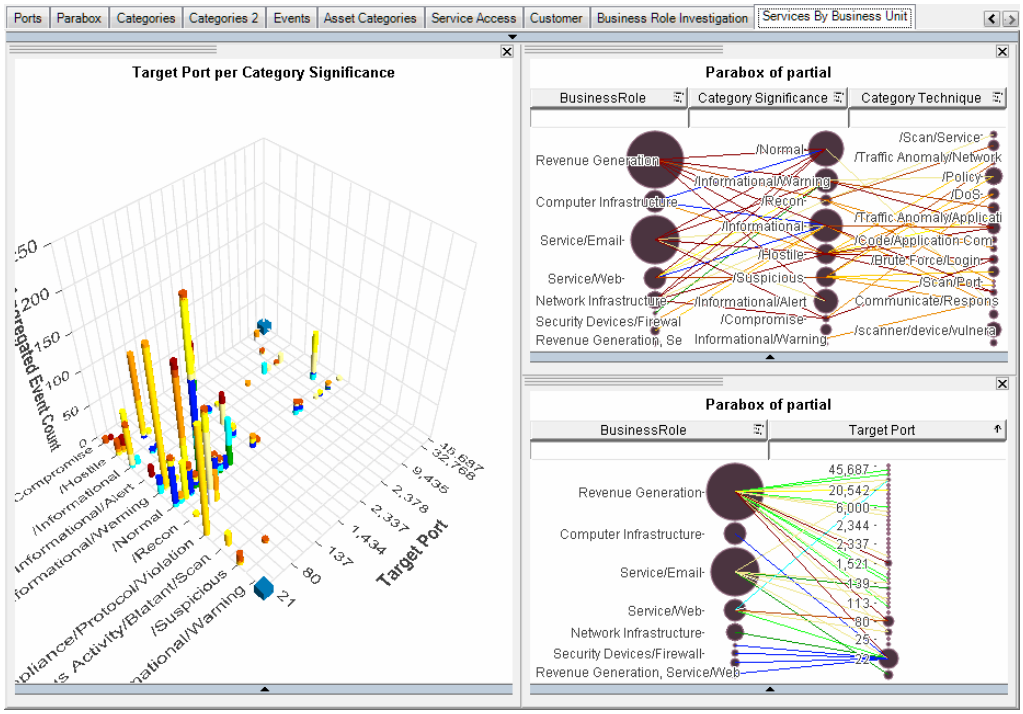


Services by Business Unit Tab

The Services by Business Unit tab contains three charts.

- **Category Significance multiscape**: Shows event counts by category significance and target port.
- **Business Role and Category parabox**: Shows the business role as it relates to category significance and technique.
- **Business Role and Target Port parabox**: Shows the business role and the target port. Use these to detect interactions, such as DOS attacks. For example, if you select a revenue-generating system, you can see types of applications that were being used on these systems, which can give you insight into

unauthorized use.



Chapter 8: Interactive Discovery Use Cases

The data files shipped with ArcSight Interactive Discovery contain sample data you can use as a tutorial to learn how to use ArcSight Interactive Discovery to discover new trends in your security data and create effective reports. This chapter walks you through some use cases to demonstrate how to use the Interactive Discovery exploratory tools and build a report.

Business Case for Interactive Discovery

Interactive Discovery enables you to present data you have collected about your network security enterprise and tailor it to different audiences. For example, you can export Interactive Discovery pages into web pages, PDF files, Microsoft Word documents, and PowerPoint presentation slides.

These additional features in this release assist you in those communications:

- The Flight Recorder
- Animation
- Data Export

The Flight Recorder

The Flight Recorder feature can be used to record all actions and selections taken in AID. It also provides the following:

- A place to collect observations by adding notes.
- Playback of previously taken actions,either in the same session on the same data or in a later session with updated data.
- Bookmarks, which may be reused in the future or shared with others.

To display the Flight Record, in the **View** menu, select **Flight Recorder.** (Flight Recorder is not displayed by default.)

Most actions are recorder by Flight Recorder automatically. Recorded actions have a one-line summary. Additional details can be displayed by toggling the gray arrow on the left.

For more about Flight Recorder, see the AID product help.

The Flight Recorder greatly enhances the Bookmark functionality found in previous versions of the product.

Animation

The animation feature enables you to visualize events in motion through time. You can choose the field to animate on.

To view the animation toolbar, click **View > Toolbars > Animate**, and then choose the appropriate fields from the drop-down lists.

For more information about animation, consult the AID product help.

Data Export

In the process of an investigation, you may want to export only the selected events in your project for further analysis or evidence.

To export selected data,

1. Click **File > Export Data**.
2. On the **Export Data dialog**, select the **Export Format**, Comma delimited (*.csv).
3. Under **Export Data**, choose **Selected**.
4. Click **OK**.

About Selection Tools

Interactive Discovery enables you to select one or more elements in a chart.

- To select a single element, click once on the element.
- To select multiple elements, click and drag over the elements you wish to select.
- To mask out the other elements on the screen, right-click your selection and choose one of the following options (or click the corresponding button in the toolbar):

Option	Description
Select all	Clears all previous selections and restores all data to the .
Unselect all	Unselects all data from the so you can choose the few you want.
Toggle Selection	Switch between Select All and Unselect All s.

Option	Description
Exclude selected	Removes the selected elements in the data .
Exclude Unselected	Removes the unselected elements in the data .
Restore excluded	Re-displays all excluded elements, whether they are selected or unselected.
Undo/ Redo	Click Undo to undo changes one at a time. Click Redo to redo changes one at a time.

When you select an element in one chart, that element is selected in all the charts on all the pages. Because each chart displays the data from a different perspective, this is how you can explore all the properties related to a data element.

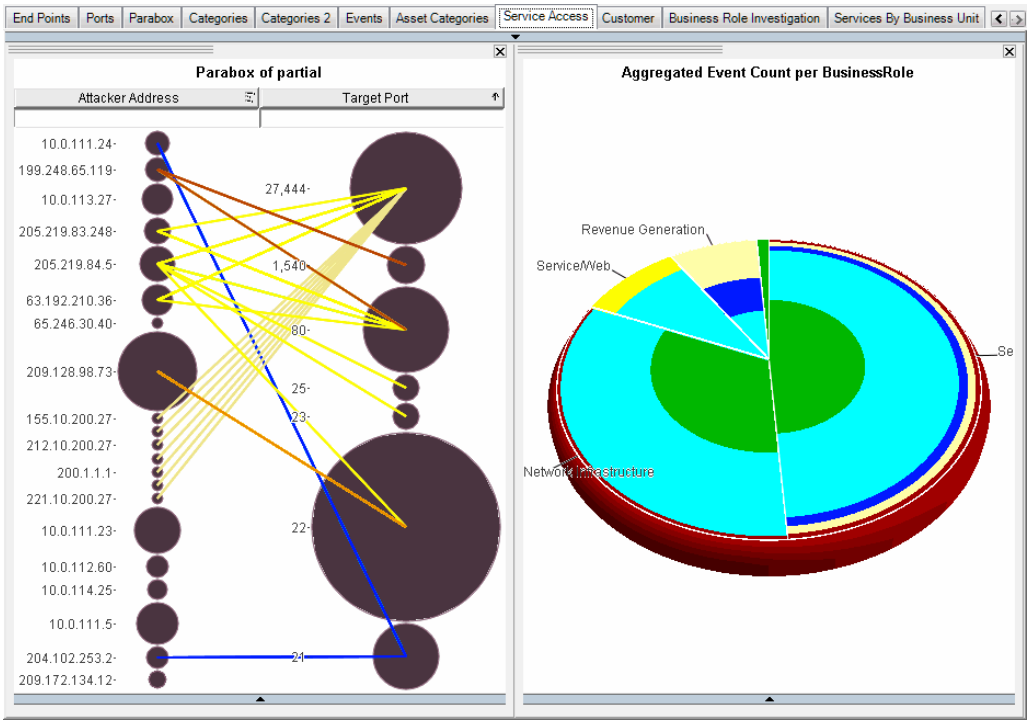
Use Case 1: Explore Security Data on Port 23

The first strategy you can use to investigate data is to click through the tabs.

Start with known vulnerabilities, such as traffic on port 23, the port used for telnet plain text traffic. Passwords go through on this port in plain text, so no users should be using it. Services, however, often use this port.

The Attacker Address and Port chart on the Service Access tab (from the AID_Schema project) shows attacker addresses on one side and the target ports on the other. Click on port 23 to select only the traffic targeting port 23. This highlights the traffic on port 23 in the other 13 tabs, which enables you to explore:

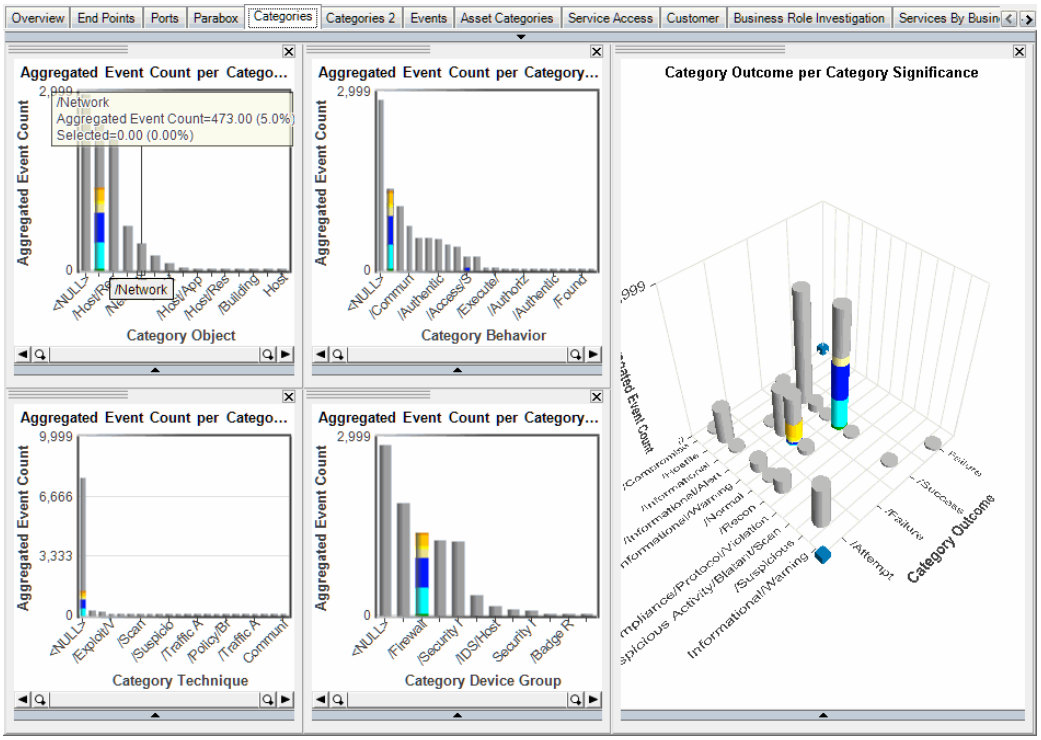
- Which systems reported the events (Over, Parabox)
- What systems that traffic targets (End Points, Parabox, Service Access)
- The business unit of the systems involved (Services by Business Unit, Business Role investigation)
- The category outcome of the events, such as success, failure, attempt (Categories, Parabox)
- The category significance of events, such as normal, suspicious, hostile (Over, Categories, Parabox)



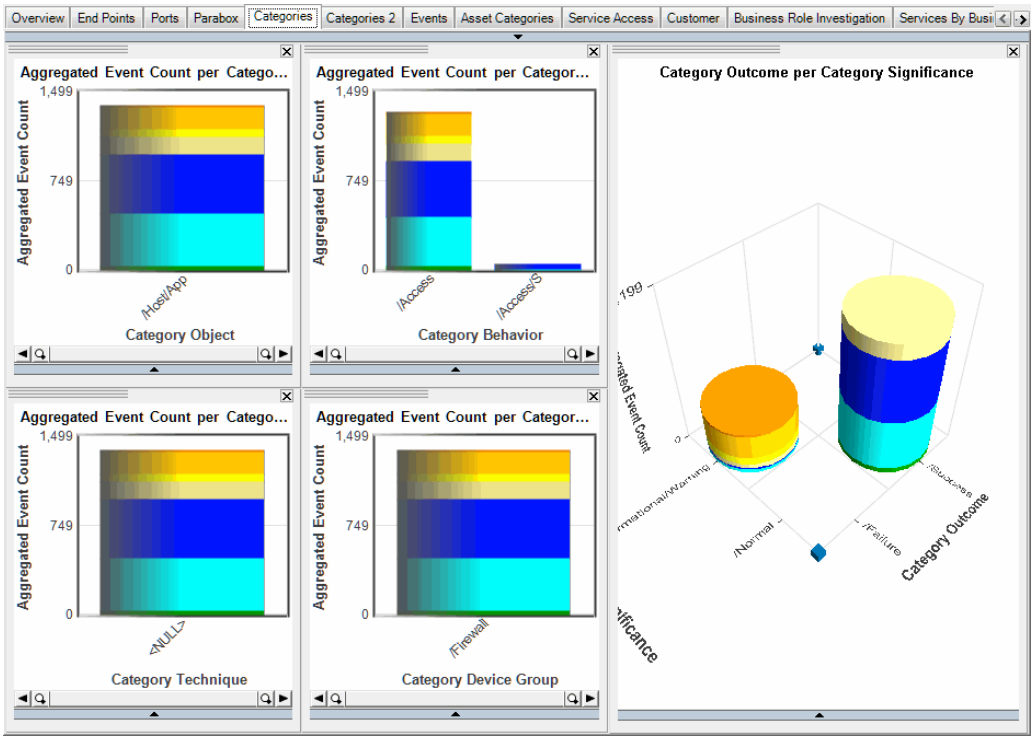
Use Case 2: Analyze Security Data from the Firewall

One common security scenario to explore is firewall activity. (This use case is specific to the ESM project only.)

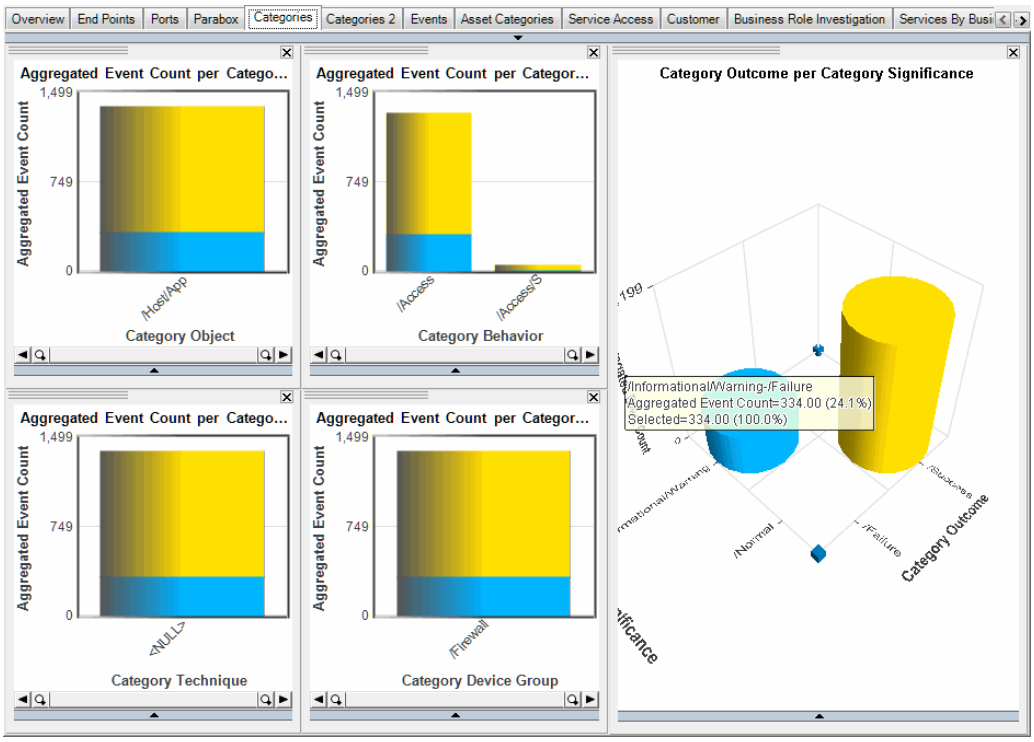
1. On the Categories tab, go to Aggregated Event Count per Category Device Group.
2. Click on the Firewall bar of the bar chart to select all firewall events.



3. Right-click the Firewall bar and select Exclude Unselected (or click the Exclude Unselected button on the toolbar) to remove unrelated events.

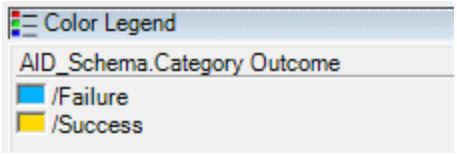


4. To see which events succeeded in passing packets through the firewall and which events failed (were blocked by the firewall), go to the Color By drop-down menu in the toolbar and select **Color Scale by Priority** and **Color by: Category Outcome.**



5. To see what the colors represent, select **View > Color and Selection Legends** from the top menu

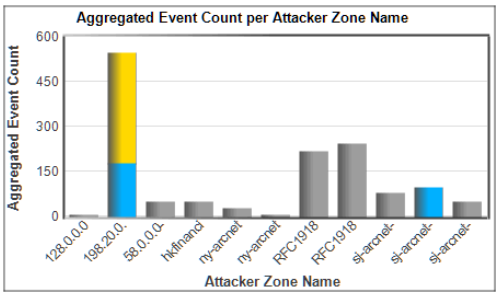
bar. Blue indicates failures (packets blocked by the firewall) and yellow indicates successes.



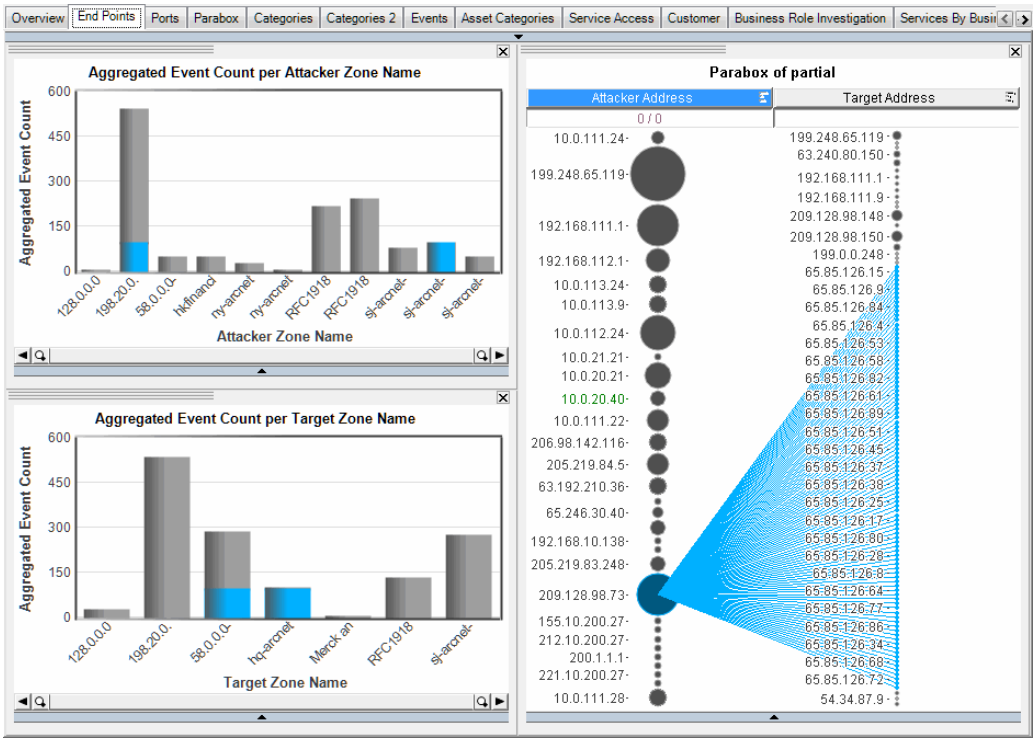
6. Click the **End Points** tab. The **Attacker/Target Address** chart on the right shows all the sources and destinations involved in the firewall success and blocks. The attacker address 209.128.98.73 circled below has a fan of many blue lines, which indicates many failures on many different systems. A pattern like this indicates potential malicious behavior.

The top attacker address, 199.248.65.119, connects to a few systems, and they were successes. The combination of these two patterns indicates a system that tries and fails many times, and then has successful connections on other targets. Because the same system has this pattern of failures, the successes are suspect.

7. You can break down this further by selecting columns from the Aggregated Event Count per Attacker Zone Name bar chart. Hold the shift key and click the two bars that contain blue: `198.20.0.0 - 222.255.255.255` and `sj-arcnet-dmz`. This shows which zones are involved in the failed connection attempts.
8. Click one bar, then hold the shift key and click the other bar in the Aggregated Event Count per Attacker Zone Name bar chart that contain failed connections (blue) to show which zones are involved in the failed connections.

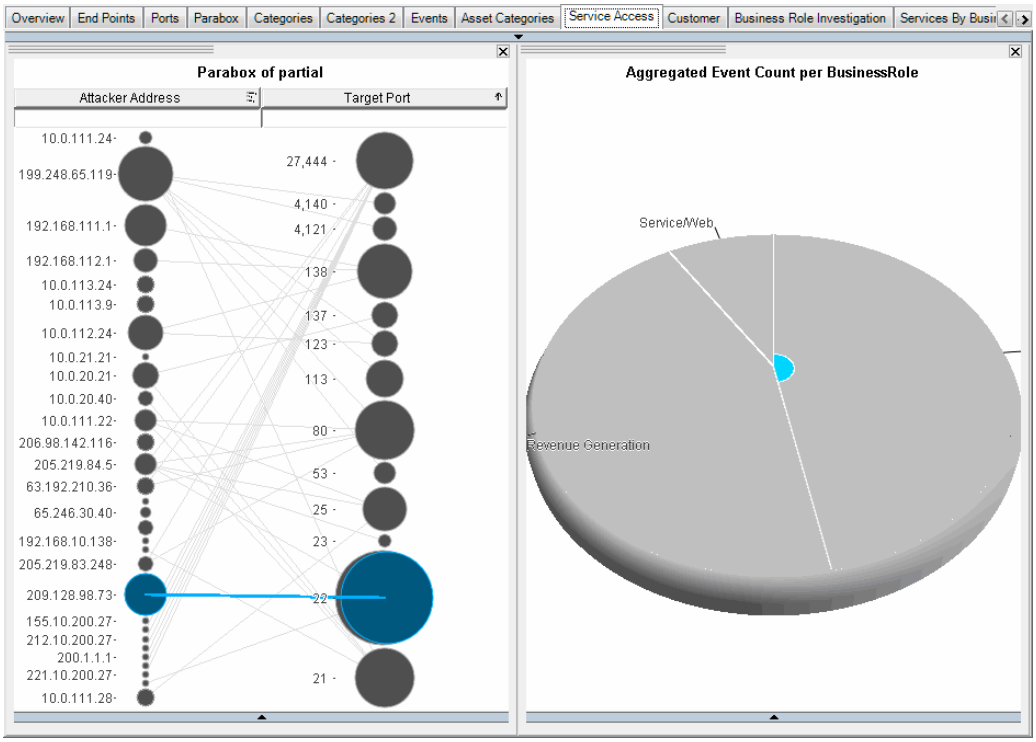


9. Next, investigate which ports the malicious attacker address connected to. Click the malicious attacker node to select just that activity. This highlights these connections in the other pages.

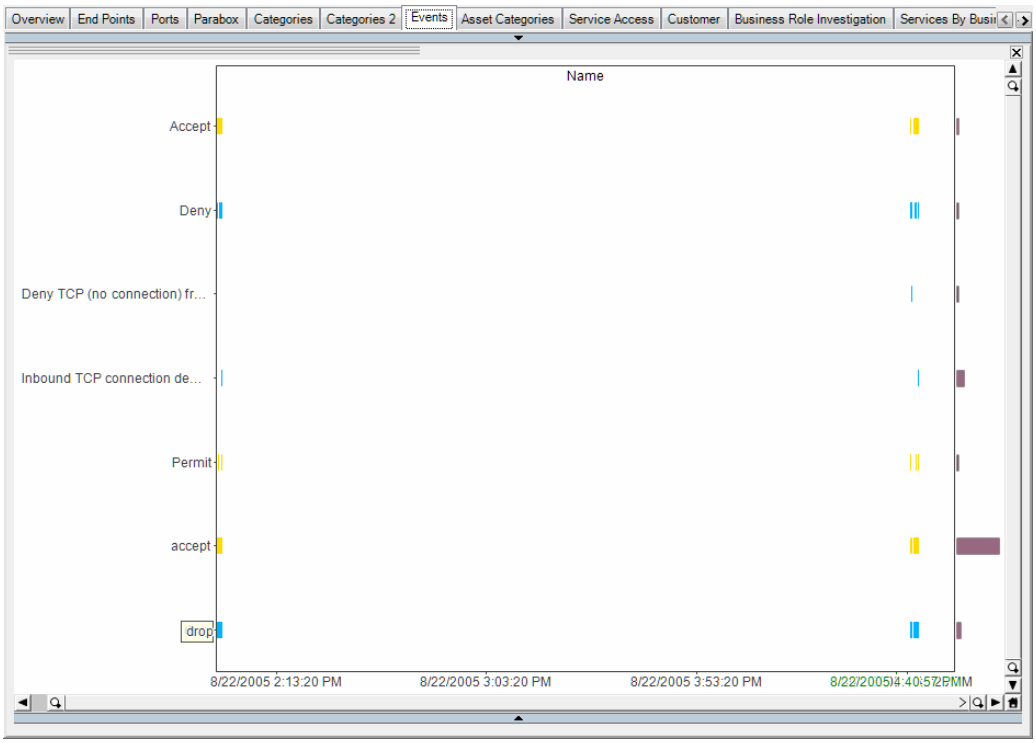


10. Click the Service Access tab. This shows the ports to which the malicious attacker has connected. According to the data, it was using only one port on different systems. This indicates that it could be a worm, which probes systems for the same port. On the other hand, if the target port that is denying service requests is a web server, it may indicate a problem with the web server.

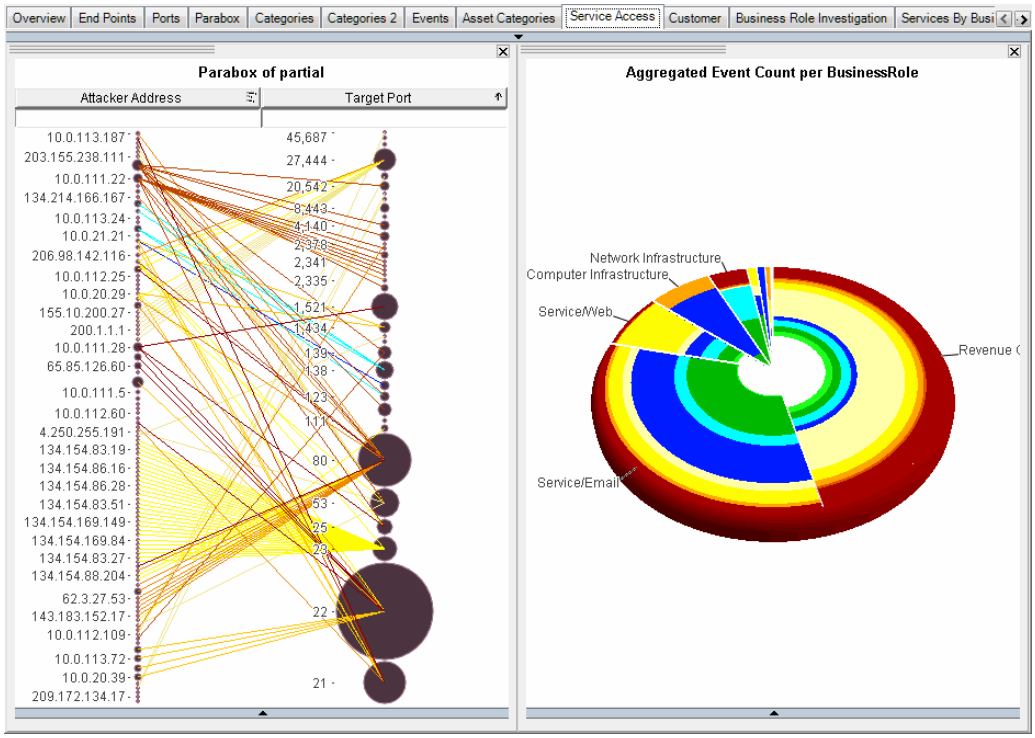
    See below: The attacker was probing different systems for port 22.



11. Click the Events tab. This shows all the event names over time. Here you look for gaps in activity. This shows a significant gap in activity, which could indicate a serious problem.



12. Go back to the **Service Access** tab and click the **Select All** toolbar button ( ) to include everything again. You may see other trends here, such as multiple port scans, which would be indicated by several fans from the attacker address column to the target port column.



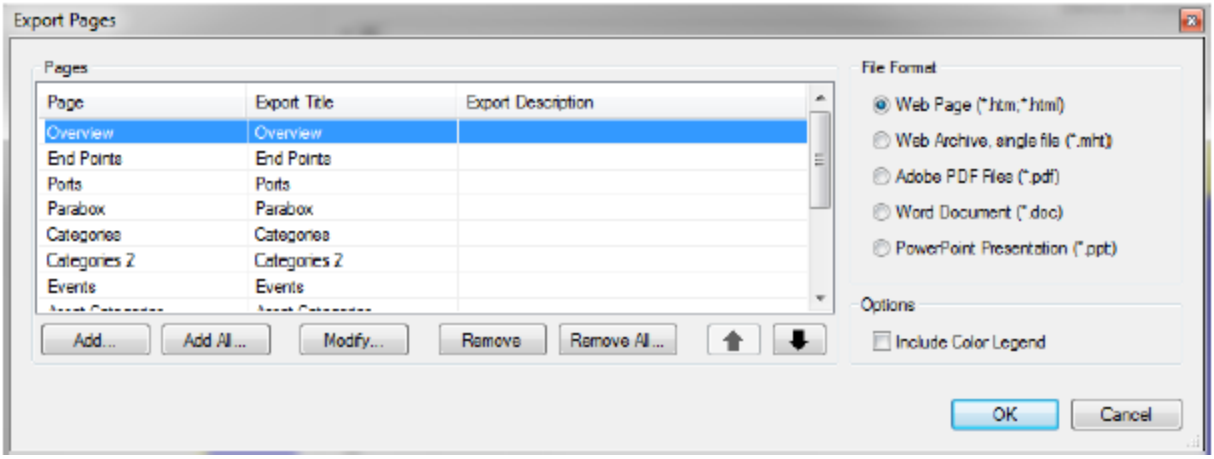
You can take the same approach to investigate attacks: look at category significance and look for events categorized as hostile.

Use Case 3: Export Pages to a Presentation

Once you have created your pages and selected the events you are visualizing, you can re-order them before exporting them to a web page, web archive, Adobe PDF file, Microsoft Word document, or PowerPoint file as a presentation.

To export one or more pages to a presentation:

1. Click **File | Export Pages**.



2. In the **Export Pages** dialog, click **Add...**
3. In the **Page Export** dialog, select a page from the **Pages** drop-down list. Optionally, add a title and description and click **OK**.
4. Continue adding pages as needed, or click **Add All** to add all pages to the export.
5. Under **File Format**, choose an output file format for the presentation.
6. Under **Options**, select **Include Color Legend**. The legend clearly communicates what the colors in your presentation represent.
7. Click **OK.** The export is saved and a message is displayed confirming the presentation save.

Appendix A: AID_Schema

This appendix lists the event fields contained in the ESM and Logger schemas. Fields present in each AID schema are indicated by “Yes” in the corresponding columns.

> The Logger schema also includes a field called Non-cef Raw Message which is automatically added during an export. It cannot be manually added or selected.

For a description of the ESM event groups, see "The Event Schema" in *ESM 101* on Protect 724.

Event Group	Event Field	Type	ESM AID_Schema	Logger AID_Schema
Event (root)	Aggregated Event Count	Integer	Yes	
	Application Protocol	Text	Yes	
	Base Event Count			Yes
	Bytes In	Integer	Yes	
	Bytes Out	Integer	Yes	
	Correlated Event Count	Integer	Yes	
	Customer Name	Text	Yes	
	End Time	DateTime	Yes	
	Event Time			Yes
	External ID			Yes
	Logger			Yes
	Name	Text	Yes	Yes
	Transport Protocol	Text	Yes	Yes
	Vulnerability Name	Text	Yes	
Attacker	Attacker Address	Text	Yes	
	Attacker Geo Latitude	Double	Yes	
	Attacker Geo Longitude	Double	Yes	

Event Group	Event Field	Type	ESM AID_Schema	Logger AID_Schema
	Attacker Port	Integer	Yes	
	Attacker Zone Name	Text	Yes	
Category	Category Behavior	Text	Yes	Yes
	Category Device Group	Text	Yes	Yes
	Category Object	Text	Yes	Yes
	Category Outcome	Text	Yes	Yes
	Category Significance	Text	Yes	Yes
	Category Technique	Text	Yes	Yes
Device	Device Action	Text	Yes	
	Device Address	Text	Yes	
	Device Event Class ID	Text		Yes
	Device Product	Text	Yes	Yes
	Device Vendor	Text	Yes	Yes
	Device Version	Text		Yes
	Device Zone Name	Text	Yes	
File	File Name	Text	Yes	
	Request URL	Text	Yes	
Target	Target Address	Text	Yes	
	Target Geo Latitude	Double	Yes	
	Target Geo Longitude	Double	Yes	
	Target Port	Integer	Yes	
	Target Zone Name	Text	Yes	
Threat	Priority	Integer	Yes	Yes

Event Group	Event Field	Type	ESM AID_Schema	Logger AID_Schema
	Relevance	Integer	Yes	
	Severity	Integer	Yes	
	Criticality of Asset	Text	Yes	
	Business Role	Text	Yes	
Source	Source Address	Text		Yes
	Source Host Name	Text		Yes
	Source Port	Integer		Yes
	Source Translated Address	Text		Yes
	Source User ID	Text		Yes
	Source User Name	Text		Yes
	Source Zone Name	Text		Yes
	Source Zone URI	Text		Yes
Destination	Destination Address	Text		Yes
	Destination Dns Domain	Text		Yes
	Destination Host Name	Text		Yes
	Destination Port	Text		Yes
	Destination Translated Address	Text		Yes
	Destination User ID	Text		Yes
	Destination User Name	Text		Yes
	Destination Zone Name	Text		Yes
	Destination Zone URI	Text		Yes

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 Project Guide (ArcSight Interactive Discovery 6.7.2)

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!