

# **ArcSight Interactive Discovery™ Projects User's Guide**

---

For ArcSight Interactive Discovery  
Version 5.6

August 24, 2012



## ArcSight Interactive Discovery™ Projects User's Guide For ArcSight Interactive Discovery Version 5.6

Copyright © 2012 Hewlett-Packard Development Company, LP. All rights reserved.

Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

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

This document is confidential.

### Revision History

Date	Product Version	Description
08/24/2012	AID v5.6	Update for ArcSight Interactive Discovery v5.6

### Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	<a href="http://support.openview.hp.com">http://support.openview.hp.com</a>
Protect 724 Community	<a href="https://protect724.arcsight.com">https://protect724.arcsight.com</a>

# Contents

---

<b>Chapter 1: About ArcSight Interactive Discovery</b>	<b>5</b>
How Interactive Discovery Works	5
Audience	6
<b>Chapter 2: Installing Interactive Discovery</b>	<b>7</b>
Installation Overview	7
Operations Overview	8
What's in the Download	8
System Requirements	9
Installation	10
Installing Interactive Discovery	10
Extracting the Content Pack	11
Importing the Interactive Discovery package into ArcSight	11
Verify Successful Content Import	12
Uninstalling Interactive Discovery	12
<b>Chapter 3: Loading Data</b>	<b>13</b>
Focused Reports Included with Interactive Discovery	13
Generating Interactive Discovery Data Files	15
Step 1: Run an Interactive Discovery Focused Report	15
Step 2: Save Report to Interactive Discovery	16
Step 3: Open Project in Interactive Discovery	16
Building a Focused Report	17
Scheduling a Focused Report	17
<b>Chapter 4: Navigation Overview</b>	<b>19</b>
<b>Chapter 5: Interactive Discovery Full Project</b>	<b>21</b>
Event List Tab	21
Overview Tab	22
Attacker Tab	23
Attacker Details Tab	24
Target Tab	25
Target Details Tab	26

---

Events Tab .....	27
Categories Tab .....	28
Categories (Continued) Tab .....	29
Category Significance Tab .....	30
Category Time Tab .....	31
Asset Categories Tab .....	32
Business Unit Tab .....	33
Workflow Tab .....	34
Customer Tab .....	35
<b>Chapter 6: Interactive Discovery Partial Project .....</b>	<b>37</b>
Overview Tab .....	37
End Points Tab .....	38
Ports Tab .....	39
Parabox Tab .....	40
Categories Tab .....	42
Categories 2 Tab .....	43
Events Tab .....	44
Asset Categories Tab .....	45
Service Access Tab .....	46
Customer Tab .....	47
Business Role Investigation Tab .....	48
Services by Business Unit Tab .....	49
<b>Chapter 7: Interactive Discovery Use Cases .....</b>	<b>51</b>
Business Case for Interactive Discovery .....	51
About Bookmarks .....	51
About Selection Tools .....	52
Use Case 1: Explore Security Data on Port 23 .....	53
Use Case 2: Analyze Security Data from the Firewall .....	54
Use Case 3: Export Bookmarks to a Presentation .....	59
<b>Appendix A: Full and Partial Schemas .....</b>	<b>61</b>
<b>Index .....</b>	<b>65</b>

# About ArcSight Interactive Discovery

ArcSight™ Interactive Discovery is a plug-and-play software utility that augments 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.

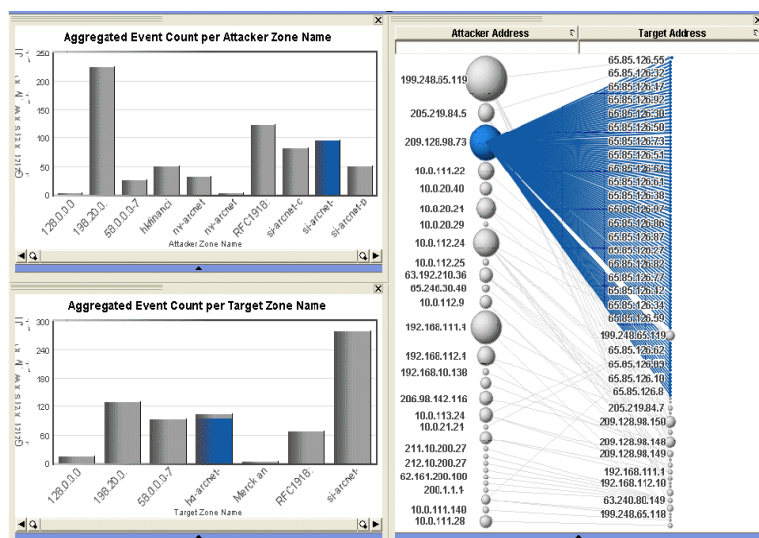
Use Interactive Discovery to:

- 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

Interactive Discovery operates on data exported from special ArcSight reports and filters in the ArcSight Content Pack. These reports interact directly with Interactive Discovery.

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.



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 users with Console access 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

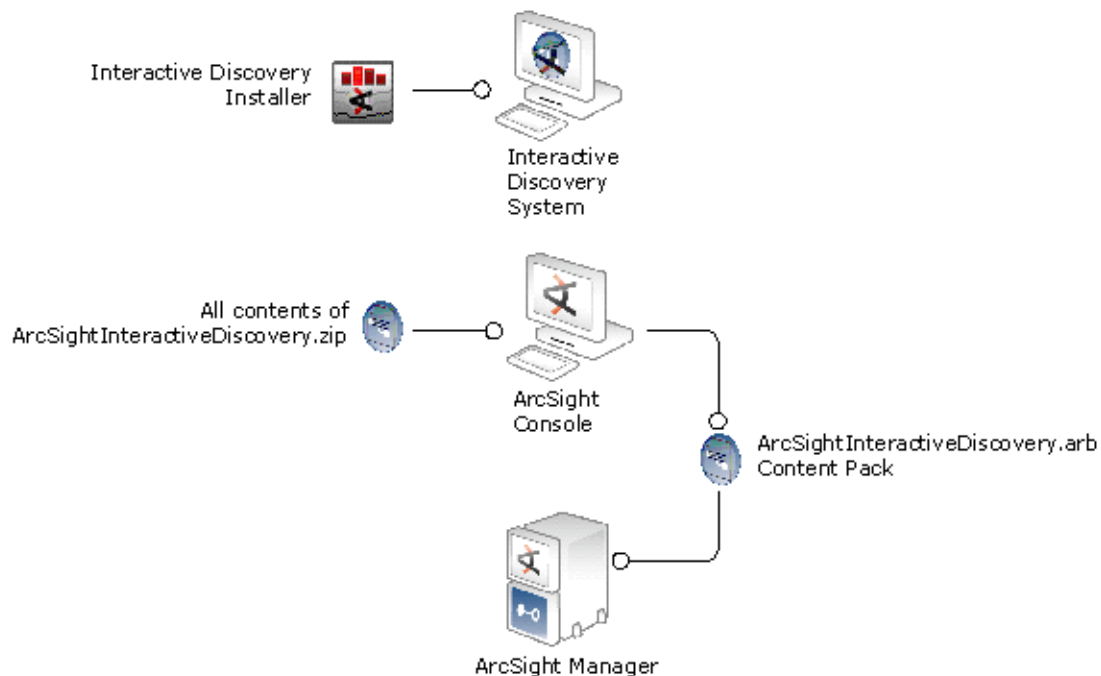
# Installing Interactive Discovery

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 CPU. 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.

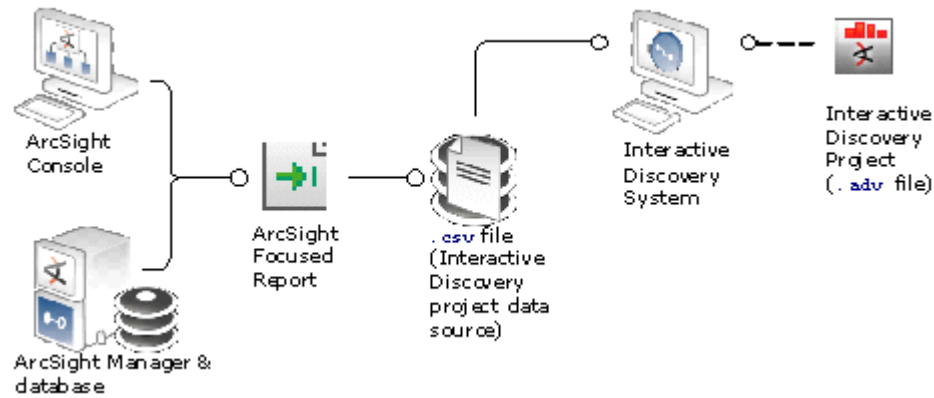
The installation consists of an installation program and a ZIP file containing the ArcSight Content Pack. Run the installation on the Interactive Discovery system, and extract the contents of the ZIP file (the [ArcsightInteractiveDiscovery.arb](#) content pack file) to the Console, which might or might not be on the same computer.



The content package goes on the ArcSight Console and is propagated to the Manager.

## 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 an ArcSight Focused Report. This means that the data itself is not contained in the ADV file, but 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 and the CSV file it generates. 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.

Interactive Discovery ships with content available with two types of schemas: partial and full. See [Appendix A, Full and Partial Schemas, on page 61](#) for the data fields included in each schema.

The partial 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.

The full schema contains data for all the event fields contained in the ArcSight event schema. Use the full schema if you need data points not contained in the partial schema. The full schema may put more of a burden on system resources, because it contains more data.

## What's in the Download

The Interactive Discovery download is called [ArcSightAID.zip](#). It contains 19 files, many of which the installer uses. The two essential files you use during installation are:

- [setup.exe](#) — the application installer
- [AID\\_Content.zip](#) — the ArcSight content pack, sample data, and project files



The content pack ZIP file ([AID\\_Content.zip](#)) contains the following files:

File	Description
ArcSight Interactive Discovery.arb	<p>You copy this ArcSight package file to the Console, from which you import it to the Manager. The ARB file contains the reports, filters, and focused reports required to output data for consumption by Interactive Discovery.</p> <p>The content of the ARB is described in <a href="#">“Focused Reports Included with Interactive Discovery” on page 13</a>.</p>
ArcSight_Full.adv	Provides access to the full schema in Interactive Discovery.
ArcSight_Partial.adv	Provides access to the partial schema in Interactive Discovery.
full.csv	<p>The project <a href="#">ArcSight_Full.adv</a> uses this file as its data source. As delivered this is a sample data file that contains the full schema of data output. After installation, you can use it to test the functions of ArcSight Interactive Discovery.</p> <p>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.</p>
partial.csv	Same as above, except it is for partial schema.
full.ini	<p>The INI files that contain initialization settings for the *.csv data source file of the same name.</p> <p>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. The content of the INI files for the ArcSight projects is the same for both full and partial CSV files. For example, for custom_full.csv, use custom_full.ini.</p> <p>Place the INI file in the same folder as its CSV file.</p>
partial.ini	


## System Requirements

Interactive Discovery can only be installed on Windows operating systems. The following minimum requirements are recommended for optimum performance:

System	Requirement
Operating System (Supported on the en-us locale)	<ul style="list-style-type: none"> <li>• Microsoft Windows XP SP1</li> <li>• Microsoft Windows Vista 32 or 64</li> <li>• Microsoft Windows 7 32 or 64</li> <li>• Microsoft Windows Server 2003 SP1</li> <li>• Windows Server 2008.</li> </ul>
Browser	Internet Explorer 7 or 8

System	Requirement
Hardware	<ul style="list-style-type: none"> <li>Any current, business-focused PC or laptop, excluding computers with low-end, entry level processors.</li> <li>2 GB of RAM or greater (See Note below). At least 2GB is required for larger volumes of data, about 750K rows.</li> <li>Graphics display processor with at least 256 MB of video RAM</li> <li>Either shared or dedicated video RAM (be sure to use the most recent drivers for the video processor)</li> <li>Video display resolution of 1024 x 768 or greater</li> <li>Video display color depth of 16 million colors</li> <li>CD-ROM drive</li> <li>Mouse or compatible pointing device</li> </ul>
ESM	See the ArcSight Interactive Discovery Readme file or Release Notes.

---



For a given data set, performance is dependent on:

- 1) Amount of RAM
- 2) Processor speed
- 3) Processor architecture/technology

The amount of RAM required depends on the number of rows and fields and the type of data.

For best results do not install ArcSight Interactive Discovery on the same machine as an ESM Manager.

## Installation

This topic covers unzipping the ArcSight Interactive Discovery package and installing or copying the included files to the appropriate systems.

### 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 listed on the previous page.
- 2 Uninstall any previous version of ArcSight Interactive Discovery.
- 3 From the HP Software Support site (<http://www.support.openview.hp.com>) download the Interactive Discovery zip file ([ArcSightAID-5.6.zip](#)) using the log-in credentials you received when you purchased ArcSight Interactive Discovery.
- 4 When you extract the AID files, the ZIP file creates and writes the files to an [ArcSightAID-5.6](#) subdirectory.
- 5 Run the Interactive Discovery executable [setup.exe](#) on the Interactive Discovery system. Follow the instructions in the installation wizard.
- 6 When the installation is complete, review the What's New section of the online help for important information regarding this release.

## Extracting the Content Pack

After unzipping [ArcSightAID-5.6.zip](#), find [AID\\_Content.zip](#) in the `\OEM\` subdirectory.

- 1 When you extract the content files, the ZIP file creates and writes the files to an [arcsight](#) subdirectory.
- 2 Verify that all the files in the ZIP file were extracted.

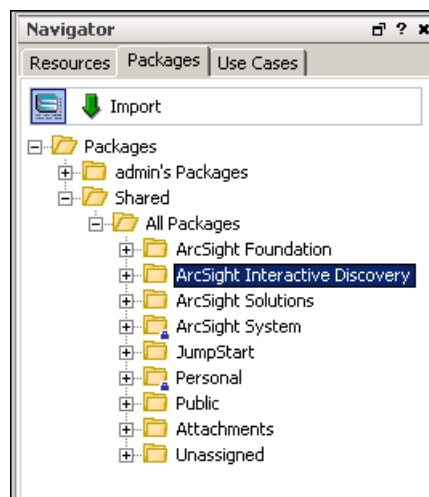
After extracting the files in this zip, you can move and copy them using these guidelines:

- 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.
- You can change the CSV file that a project uses and then save the project with a different name.
- Maintain the association between the full (or partial) ADV projects and the full (or partial) CSV files. That is, don't mix full and partial files.

## Importing the Interactive Discovery package into ArcSight

Use the ArcSight Console import capability to import the [ArcSight Interactive Discovery.arb](#) content file, as described below.

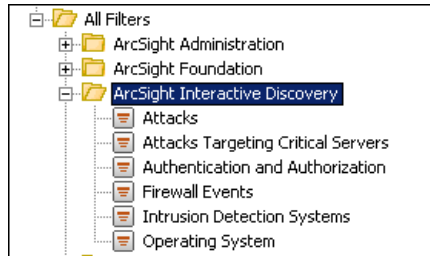
- 1 Save the [ArcSight Interactive Discovery.arb](#) content file to a network location accessible to your ArcSight Console.
- 2 Launch ArcSight Console.
- 3 In the Navigator panel, click the **Packages** tab.
- 4 Click **Import**, at the top of the Packages tab.
- 5 Access the [ARB](#) file and click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



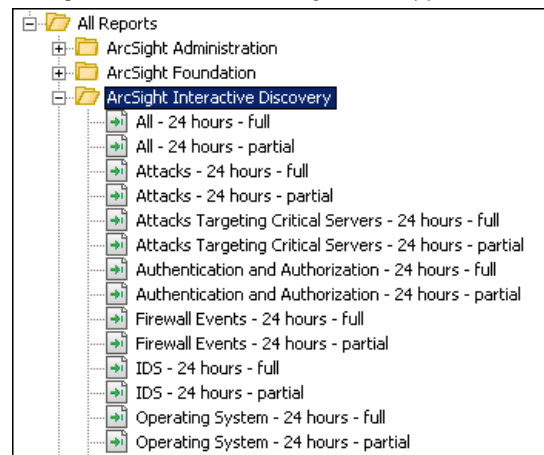
## Verify Successful Content Import

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

- 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

Note that the reports shown above are focused reports. There is also a subfolder called Templates containing Full Schema and Partial Schema base reports from which you can create other focused reports.

## Uninstalling Interactive Discovery

To uninstall Interactive Discovery:

- 1 Go to **Start > Control Panel > Programs and Features**.
- 2 Right-click on **ArcSight Interactive Discovery** and select **Uninstall**.

To uninstall the AID content from the 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**.

## Chapter 3

# Loading Data

---

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

- [“Focused Reports Included with Interactive Discovery” on page 13](#)
- [“Generating Interactive Discovery Data Files” on page 15](#)
  - ◆ [“Step 1: Run an Interactive Discovery Focused Report” on page 15](#)
  - ◆ [“Step 2: Save Report to Interactive Discovery” on page 16](#)
  - ◆ [“Step 3: Open Project in Interactive Discovery” on page 16](#)
- [“Building a Focused Report” on page 17](#)
- [“Scheduling a Focused Report” on page 17](#)

## Focused Reports Included with Interactive Discovery

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

[/All Reports/ArcSight Interactive Discovery/Templates/](#).

Template	Description
Partial 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 ArcSight Manager to the Explorer.
Full Schema	This report shows all the ArcSight event fields, that are useful for analysis. Analysis using this report might be slower due to the larger amount of data that has to be processed.

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 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 <a href="#">/All Asset Categories/System Asset Categories/Criticality/Very High</a> .
Authentication and Authorization	Shows authentication and authorization events (logins, password changes, and so on).
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 Console Navigator's **Reports** resource: [/All Reports/ArcSight Interactive Discovery...](#) All the Interactive Discovery reports filter out ArcSight internal events (self-auditing events).

Focused Report	Description
All – 24 hours – full	Compiles all events (no filters applied) in the past 24 hours using the full schema of data.
All – 24 hours – partial	Compiles all events (no filters applied) in the past 24 hours using the partial schema of data.
Attacks – 24 hours – full	Compiles all events that involve attacks in the past 24 hours using the full schema of data.
Attacks – 24 hours - partial	Compiles all events that involve attacks in the past 24 hours using the partial schema of data.
Attacks Targeting Critical Servers – 24 hours – full	Compiles all events that targeted critical servers in the past 24 hours using the full schema.
Attacks Targeting Critical Servers – 24 hours – partial	Compiles all events that targeted critical servers in the past 24 hours using the partial schema.
Authentication and Authorization – 24 hours - full	Compiles all events classified as authentication and authorization events in the past 24 hours using the full schema of data.
Authentication and Authorization – 24 hours – partial	Compiles all events classified as authentication and authorization events in the past 24 hours using the partial schema of data.
Firewall Events – 24 hours - full	Compiles all firewall events in the past 24 hours using the full schema of data.
Firewall Events – 24 hours – partial	Compiles all firewall events in the past 24 hours using the partial schema of data.

Focused Report	Description
IDS – 24 hours - full	Compiles all IDS events in the past 24 hours using the full schema of data.
IDS – 24 hours – partial	Compiles all IDS events in the past 24 hours using the partial schema of data.
Operating System – 24 hours - full	Compiles all operating system events, such as memory, buffer, and event handler messages, in the past 24 hours using the full schema of data.
Operating System – 24 hours - partial	Compiles all operating system events (such as resource failures and system reboot) in the past 24 hours using the partial schema of data.

## Generating Interactive Discovery Data Files

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

- 1 From the ArcSight Console, run one of the Interactive Discovery focused reports. You can run them as needed or set them to run daily. For instructions about how to schedule reports, see the Console online Help topic "Scheduling Tasks."



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 and time stamps.

- 2 Open the report output file and save it to c:\arcsight either as full.csv or partial.csv depending on which report you ran on the Console.

You can specify any file name, but you should use CSVs containing full data with the ADV project files for full data. Same for partial data. Including "full" or "partial" in the name can help you keep them straight.

In addition, you must save an INI file with the same name as the CSV file. The content of the INI files is the same for full and partial data.

- 3 If you have a separate Interactive Discovery machine, copy the CSV file to c:\arcsight on the Interactive Discovery machine. The CSV and its matching INI file can actually go in any folder. When you open the ADV file you can point it to the appropriate data source. To change or add data source CSV files in Interactive Discovery, select **File > Manage Data Sources**.
- 4 Open the Interactive Discovery ADV project file (ArcSight\_Full.adv or ArcSight\_Partial.adv).

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.

## Step 1: Run an Interactive Discovery Focused Report

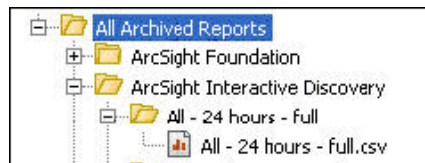
- 1 In the Navigator panel Reports resource tree, go to /All Reports/ArcSight Interactive Discovery.
- 2 Right-click the focused report you wish to run and select **Run > Report with defaults**.

- 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...  
appears 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...  
appears. 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.

If your report contains more than 100,000 lines of output, edit the report (Right-click the report's icon and choose **Edit Report**) and change the maximum number of events shown.

## Step 2: Save Report to Interactive Discovery

- 1 Save the focused report output CSV file on the local Console drive with an appropriate name indicating whether it uses full or partial data schema.
- 2 Copy the file to the Interactive Discovery system.
- 3 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. The content of full.ini and partial.ini are the same, so you can copy and rename either one.
- 4 Navigate to **All Archived Reports > ArcSight Interactive Discovery** and find the report you just ran. You should see your report saved with the date and time the report was run and the file extension CSV, as shown below.



- 5 Save the file to the local Console machine.
  - ◆ 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 c:\arcsight, where the other Interactive Discovery files are located.
- 6 If Interactive Discovery is installed on its own system, copy the CSV file from the Console to the Interactive Discovery system.

## Step 3: Open Project in Interactive Discovery

Next, open the ArcSight project in Interactive Discovery. Interactive Discovery ships with two projects:

- ArcSight\_Full.adv
- ArcSight\_Partial.adv

Which project file you open depends on which report you ran at step 1 to generate the CSV file that the project uses as its data source.

- 1 On the Interactive Discovery system, launch Interactive Discovery.



You can launch it by double-clicking `c:\arcsight\ArcSight_Full.adv` (or `ArcSight_Partial.adv`). If you do, skip to step 3.

- 2 At the Getting Started screen, select **Open Project**.
- 3 At the Open Project screen, select `ArcSight_Full.adv` or `ArcSight_Partial.adv`. Open `ArcSight_Full.adv` to load `full.csv`; open `ArcSight_Partial.adv` to load `partial.csv`.
- 4 Each ADV file remembers the absolute path to its associated CSV file. When you first open a project you might get a **Locate Missing Data File** dialog that reports the path of the CSV file it cannot find. For example,  
`C:\ArcSightAID-5.6\OEM\arcsight\full.csv`

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

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

## Building a Focused Report

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 either the Full Schema or Partial 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

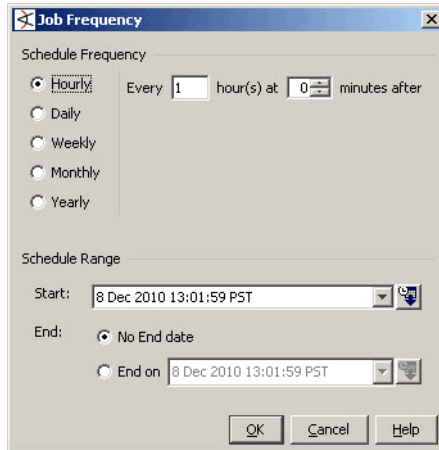
The reports are designed to run on data from the past 24 hours, so schedule the report to run daily. Once the report has run, save it as `full.csv` or `partial.csv`, and copy it to the Interactive Discovery system, as described in [“Step 2: Save Report to Interactive Discovery” on page 16](#).

- 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** to see the Job Frequency window.



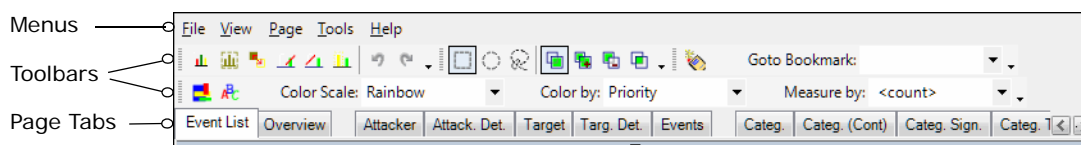
- 6 When the report has run, follow the instructions in Step 2: Save Report as "full.csv" or "partial.csv" and Copy to Interactive Discovery System as described in ["Step 2: Save Report to Interactive Discovery" on page 16](#).

## Chapter 4

# Navigation Overview

The two Interactive Discovery projects contain a set of tabs that enable you to analyze your network security data using different interactive graphics.

Follow the instructions in “[Step 3: Open Project in Interactive Discovery](#)” on page 16 to open [ArcSight\\_Full.adv](#). 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 find the tool bar for each chart or list panel by clicking the small triangle in the gray bar beneath the panel, as shown below.



You can 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 *ArcSight ESM 101*, Chapter 2, “Lifecycle of an Event through ArcSight.”

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 5

# Interactive Discovery Full Project

The full project provides a view of the full set of data using the project tabs described in this chapter. Compare these tabs to the partial project to see which views each provides and determine which will be of the most use to you for different purposes.

You can use the “full” reports provided in the package (the ARB file) to generate the data appropriate for the full project.

The full schema contains data for all the event fields contained in the ArcSight event schema. Use the full schema if you need data points not in the partial schema. The full schema may put more of a burden on system resources, because it contains more data.

## Event List Tab

The Event List tab contains one large list of all events in the data set over time. In addition, there are four filter control boxes that allow you to select which events to show. These controls allow you to filter by Priority, Criticality of Asset, Category Significance, and Category Outcome.

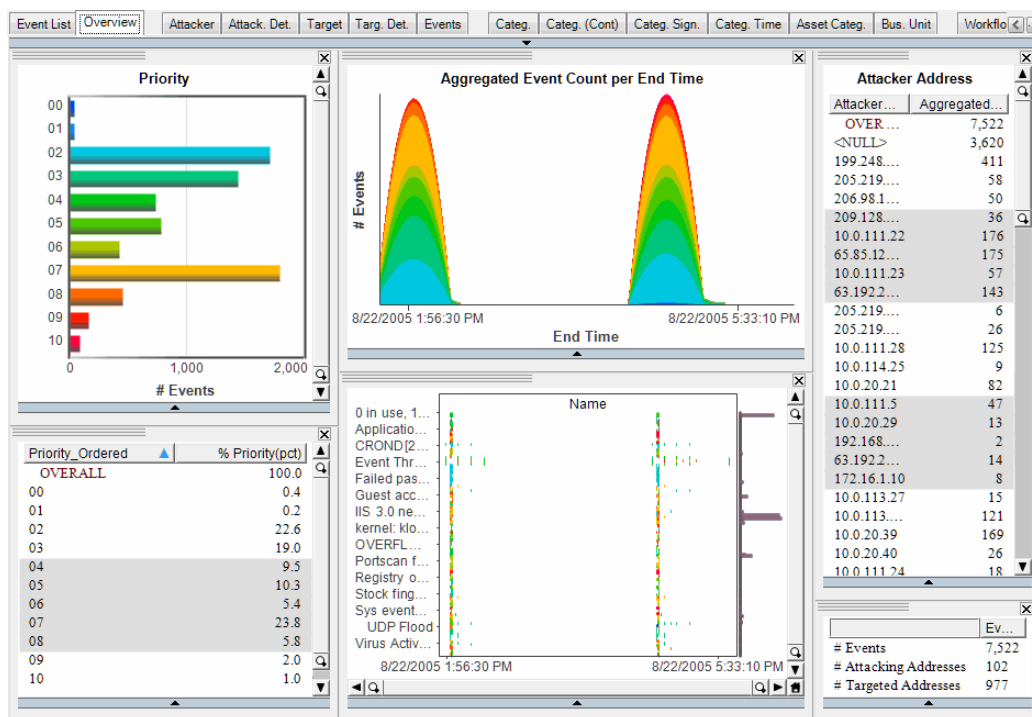
Event List/Right Click to Export

Attacker...	Attacker Z...	Attack...	Name	End Time	Targ...	Target Zon...	Target...	Category...	Category...	Criti...	Pr...
10.0.114.25	sj-arcnet-vpn	54,456	Accepted password	8/22/2005 4:44:2...	10.0...	sj-arcnet-co...	brian	/Success	/Normal	<N...	2
10.0.114.25	sj-arcnet-vpn	<NUL...	Attack From Susp...	8/22/2005 4:44:2...	10.0...	sj-arcnet-co...	<NUL...	/Attempt	/Hostile	<N...	8
10.0.114.25	sj-arcnet-vpn	54,456	Failed password	8/22/2005 4:44:2...	10.0...	sj-arcnet-co...	brian	/Failure	/Infor...	<N...	2
10.0.114.25	sj-arcnet-vpn	<NUL...	Hostile - Attempt	8/22/2005 4:44:2...	10.0...	sj-arcnet-co...	<NUL...	/Success	/Normal	<N...	6
10.0.20.21	sj-arcnet-pro...	35,072	accept	8/22/2005 4:45:5...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:5...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,541	accept	8/22/2005 4:46:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:3...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	137	accept	8/22/2005 4:45:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:1...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,540	accept	8/22/2005 4:45:3...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,541	accept	8/22/2005 4:45:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:2...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,920	accept	8/22/2005 4:45:3...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,540	accept	8/22/2005 4:45:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:1...	2069...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,548	accept	8/22/2005 4:45:3...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,548	accept	8/22/2005 4:45:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,526	accept	8/22/2005 4:45:3...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,504	accept	8/22/2005 4:45:5...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:46:0...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	4,508	accept	8/22/2005 4:45:2...	1992...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4
10.0.20.21	sj-arcnet-pro...	1,526	accept	8/22/2005 4:44:2...	1002...	198.20.0.0...	<NUL...	/Success	/Normal	Low	4

## Overview Tab

The Overview tab contains three charts and three lists.

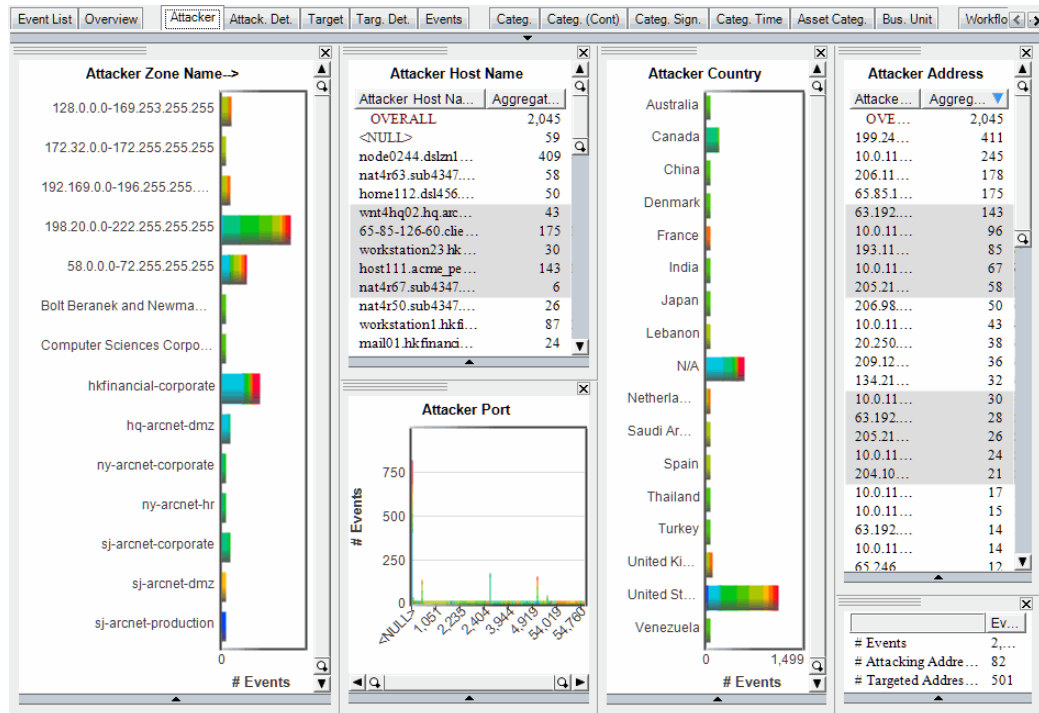
- **Count per Priority bar chart:** Shows the number of events of each priority as determined by the ArcSight threat level formula.
- **Event Count per End Time chart:** Shows number of aggregated events by end time.
- **Event Name by Time:** Shows the time distribution when each event name occurred.
- **Percentage of Events for Priority List:** Shows a list of all the different event priorities and the percentage of to total events that have this priority.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.



## Attacker Tab

The Attacker tab contains three charts and three lists.

- **Attacker Zone Name:** Shows the number of events for each attacker zone name.
- **Attacker Host Name Count:** Shows number of events from each attacker host name.
- **Attacker Port Count:** Shows the number of events from each attacker port.
- **Attacker Country Count:** Shows the number of events from each attacker country.
- **Number of Events per Attacker Address:** Shows the aggregated event count for events from each attacker address.
- **Event Counts:** Shows the total number of events and the numbers different attacking and targeted addresses.



## Attacker Details Tab

The Attacker Details tab shows information about the attacker for each event. It includes the attacker's IP address, zone, host name, port, user ID, process and service name, and other details.

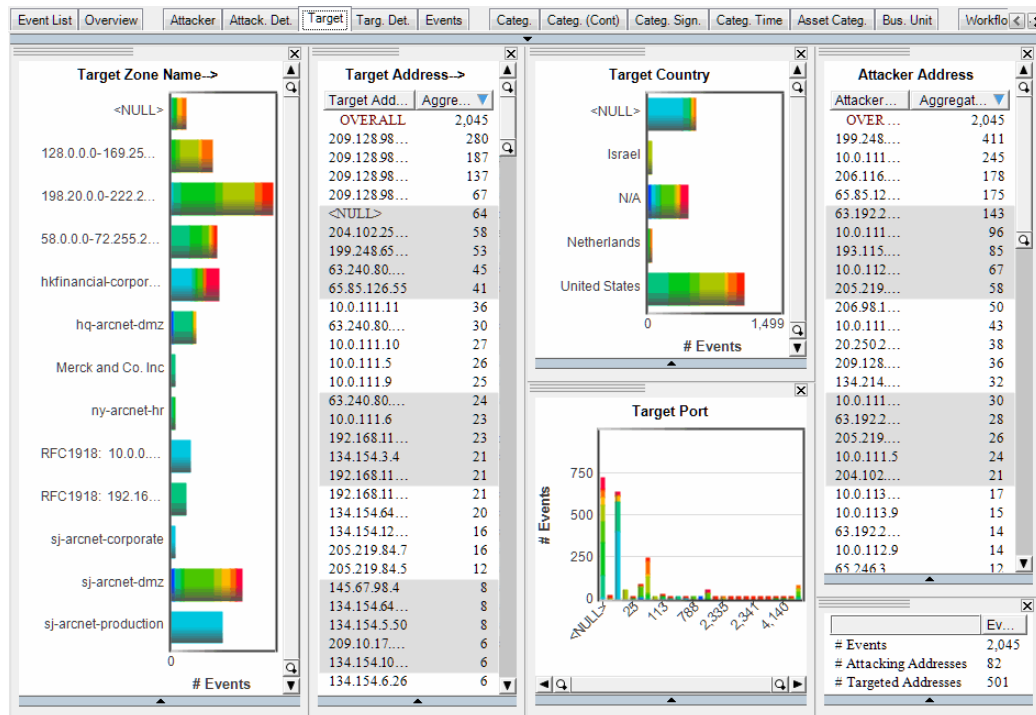
Event List	Overview	Attacker	Attack Det	Target	Targ. Det.	Events	Categ.	Categ. (Cont)	Categ. Sign.	Categ. Time	Asset Categ.	Bus. Unit	Workflow
Attacker Details//Right Click to Export													
Attacker Address	Attacker Zone Name	Attacker Host Name	Attacker Port	Attacker Geo Country Code	Attacker...	Attacker...							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	31,488	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,343	US	<NULL>	<NULL>							
206.98.142.116	198.20.0.0-222.255.255.255	home112.dsl456.mindspring.com	1,024	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,341	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,345	US	<NULL>	<NULL>							
206.98.142.116	198.20.0.0-222.255.255.255	home112.dsl456.mindspring.com	1,024	US	<NULL>	<NULL>							
200.1.1.1	198.20.0.0-222.255.255.255	somebody.in.venezuela.ve	1,024	VE	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	3,613	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,337	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,343	US	<NULL>	<NULL>							
221.10.200.27	198.20.0.0-222.255.255.255	somebody.in.china.cn	1,024	CN	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,342	US	<NULL>	<NULL>							
221.10.200.27	198.20.0.0-222.255.255.255	somebody.in.china.cn	1,024	CN	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	3,613	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,336	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,338	US	<NULL>	<NULL>							
212.10.200.27	198.20.0.0-222.255.255.255	somebody.in.denmark.dk	1,024	DK	<NULL>	<NULL>							
206.98.142.116	198.20.0.0-222.255.255.255	home112.dsl456.mindspring.com	1,024	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,344	US	<NULL>	<NULL>							
202.10.200.27	198.20.0.0-222.255.255.255	somebody.in.australia.au	1,024	AU	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,344	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,341	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,345	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,335	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,341	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,337	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,335	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,344	US	<NULL>	<NULL>							
199.248.65.119	198.20.0.0-222.255.255.255	node0244.dsln11.badguy.net	2,336	US	<NULL>	<NULL>							
212.10.200.27	198.20.0.0-222.255.255.255	somebody.in.denmark.dk	1,024	DK	<NULL>	<NULL>							
211.10.200.27	198.20.0.0-222.255.255.255	somebody.in.japan.jp	1,024	JP	<NULL>	<NULL>							



## Target Tab

The Target tab contains three charts and three lists:

- **Target Zone Name:** Shows the number of events for each target zone name.
- **Target Host Name:** Shows number of events from each target host name.
- **Target Port Count:** Shows the number of events from each target port.
- **Target Country Count Bar Chart:** Shows the number of events from each target country.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.



## Target Details Tab

The Target Details tab shows information about the target for each event. It includes the target's IP address, zone, host name, port, user ID, process and service name, and other details.

Event List	Overview	Attack	Attack Det.	Target	Targ. Det.	Events (A)	Events (B)	Categ.	Categ. (Cont)	Categ. Sign.	Categ. Time	Asset Categ.	Bus. U
Target Details													
Target Address	Target Zone Name	Target Asset Name	Target Host Name	Target Port	Target Net...	Target Geo Count...							
10.0.20.40	sj-arcnet-production	linsj103.internal	linsj103.sj1.west.arcnet.com	1,434	<NULL>	N/A							
10.0.20.40	sj-arcnet-production	linsj103.internal	linsj103.sj1.west.arcnet.com	1,434	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	20,542	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	80	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	20,542	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	53	<NULL>	United States							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	80	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	80	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	53	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	80	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	80	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	20,542	<NULL>	N/A							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	<NULL>	<NULL>	N/A							
209.128.98.149	sj-arcnet-dmz	<NULL>	w2ksj101.sj1.west.arcnet.com	<NULL>	<NULL>	United States							
209.128.98.148	sj-arcnet-dmz	wnt4sj102.external	wnt4sj102.sj1.west.arcnet.com	20,542	<NULL>	N/A							



## Categories Tab

The Categories tab gives you an idea of what's happening according to the ArcSight event categories.

The Categories tab contains three charts and two lists:

- **Event Count per Category Object:** For each category of objects (host, application, service, and so on) it shows the number of aggregated events.
- **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.
- **Event Count per Category Behavior:** For each category of behaviors (access, add, delete, execute, and so on) it shows the number of aggregated events.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.

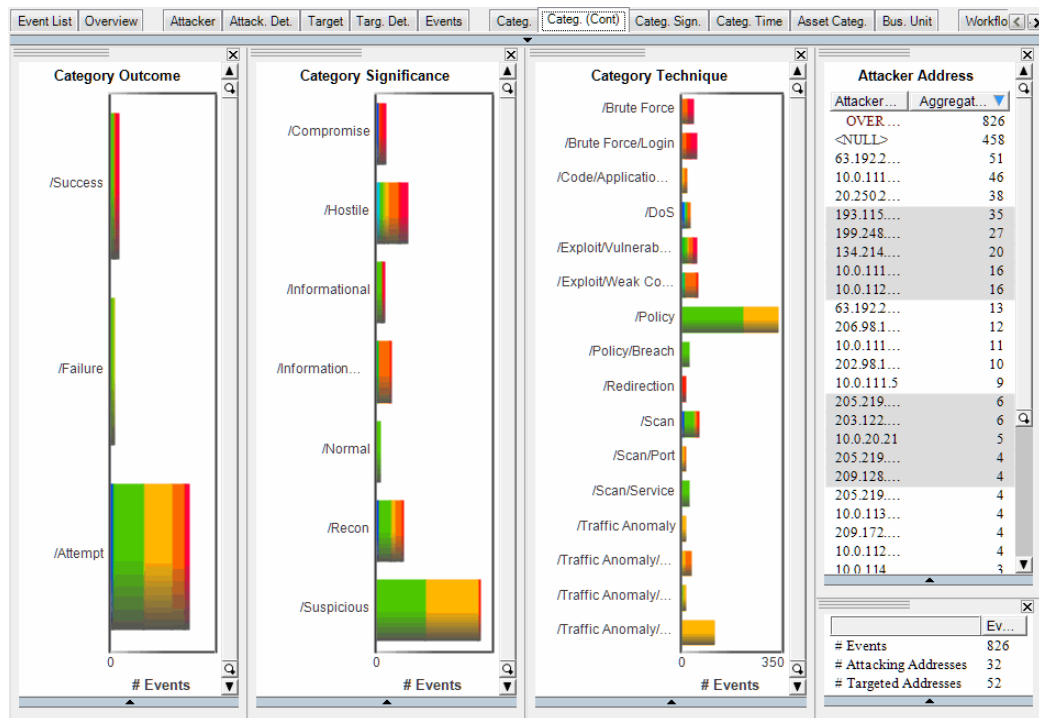


## Categories (Continued) Tab

The Categories (continued) tab contains Three more charts and two tables:

- **Event Count per Category Outcome:** For each category of outcomes (success, failure, attempt, and so on), it shows the number of aggregated events.
- **Event Count per Category Significance:** For each category of significance (hostile, normal, warning, and so on), it shows the number of aggregated events.
- **Event Count per Category Technique:** For each category of techniques (brute force, scan, redirection, and so on), it shows the number of aggregated events.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers of different attacking and targeted addresses.

Monitor this tab for gaps in activity.

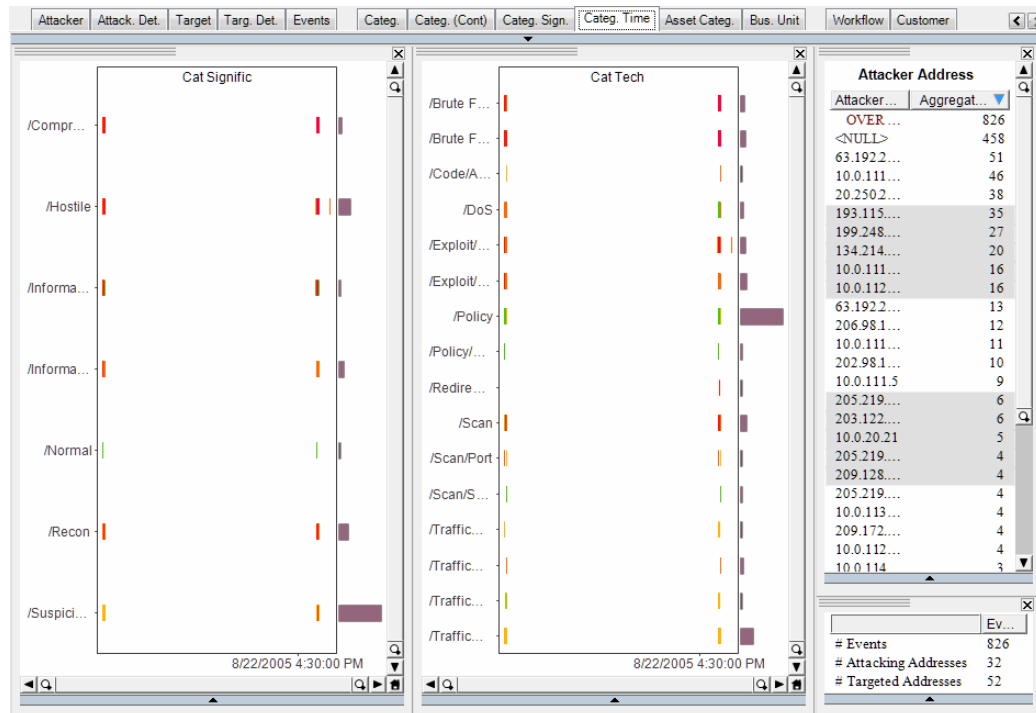




## Category Time Tab

The Category Time tab shows two charts and two lists.

- **Category Significance by Time:** For each category of significance (hostile, normal, warning, and so on) it shows a time line of when events occur ed with an indicator bar showing the relative event count for events of this significance.
- **Category Technique by time:** For each category of technique (brute force, scan, redirection, and so on) it shows a time line of when events occur ed with an indicator bar showing the relative event count for events of this technique.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.

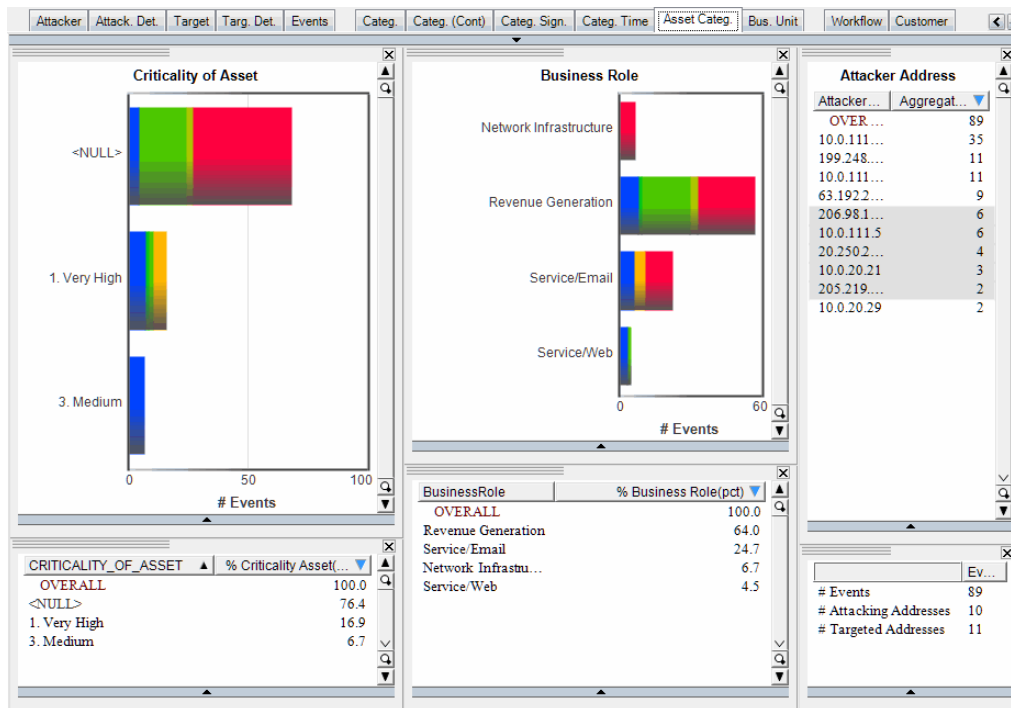


## Asset Categories Tab

The Asset Categories tab shows two charts and four lists.

- **Criticality of Assets:** Shows the percentage of events based on the asset's criticality. Asset criticality is determined by the ArcSight threat level formula.
- **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.
- **Criticality of Asset Percentage:** Lists the percentage of events for each level of criticality.
- **Business Role percentage:** Lists the percentage of events related to each business role.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.

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

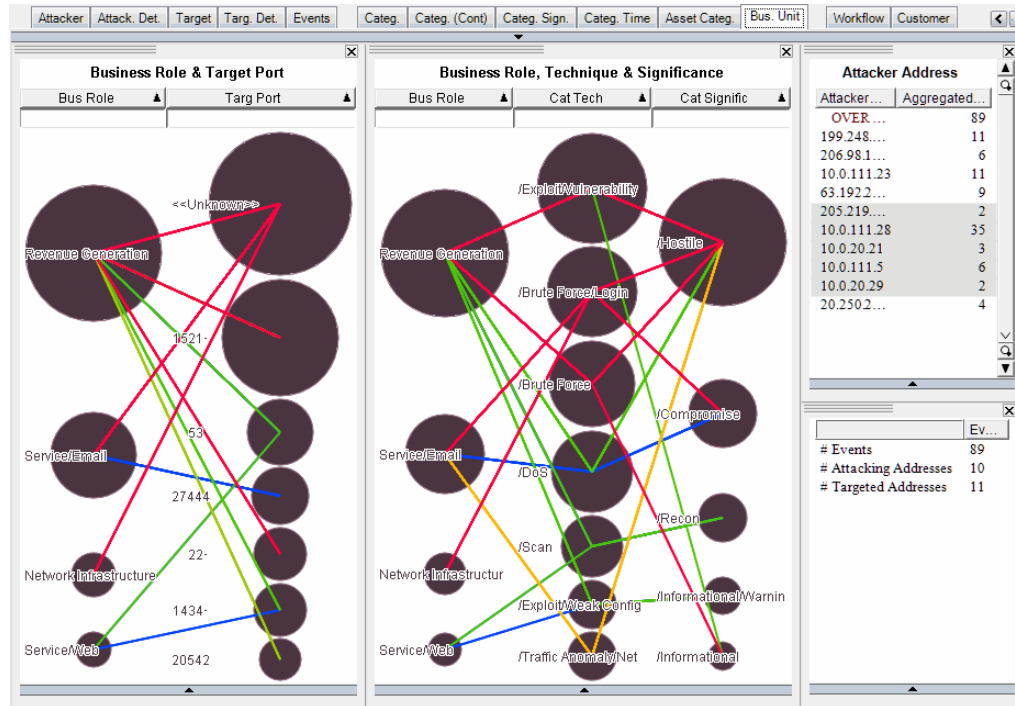




## Business Unit Tab

The Business Unit tab contains two charts and two lists.

- **Business Role and Target Port:** 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.
- **Business Role by Technique & Significance:** Shows the business role as it relates to category significance and technique.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.



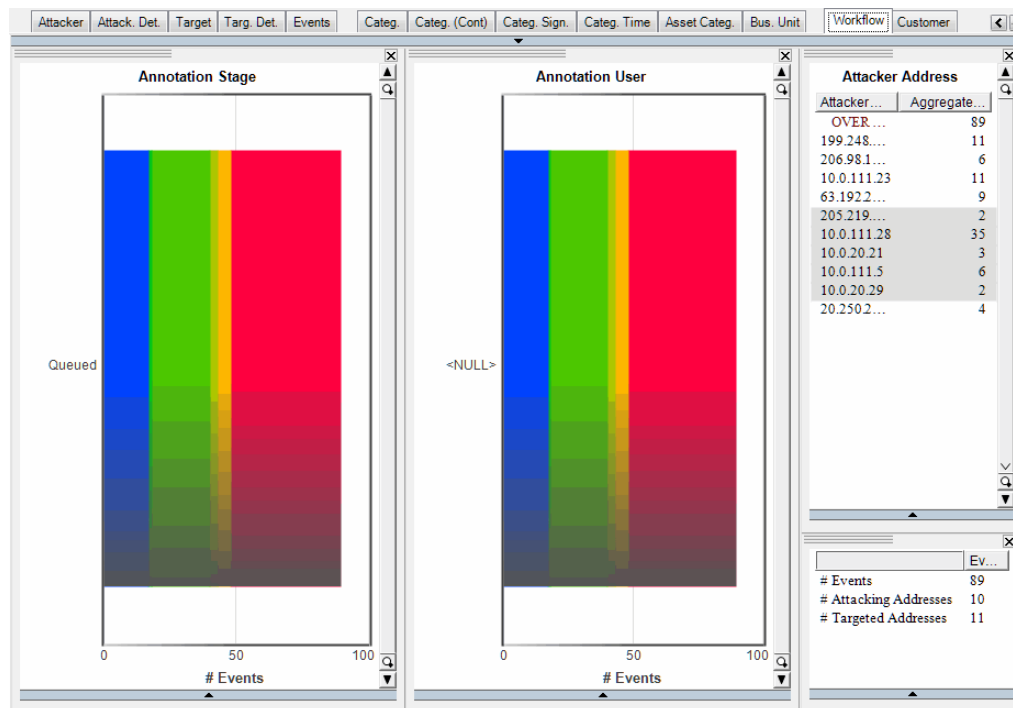
## Workflow Tab

The Workflow tab appears only in the full view project file. The example shown above is derived from a sample data set that is not shipped with the product.

This tab contains two charts and two lists:

- **Annotation Stage:** A bar chart that shows the stage to which all events are assigned. If events have not specifically been assigned to a particular user, they show up by default as being in the queued stage.
- **Annotation User:** A bar chart that shows the names of the users to whom events are assigned.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.

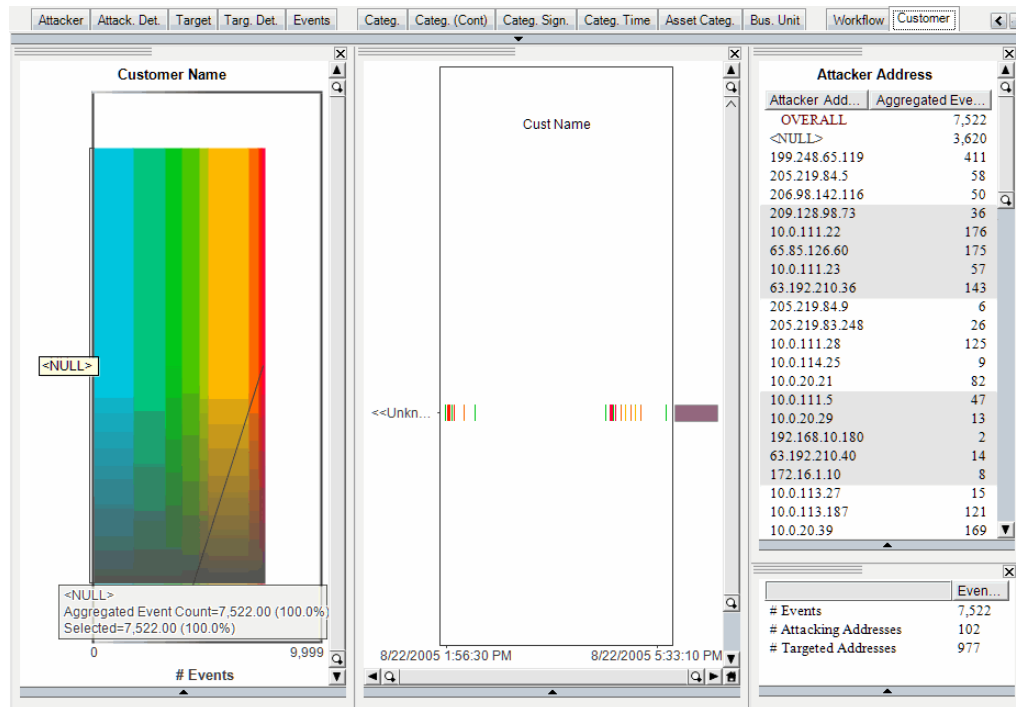
Use the views on this tab to track the investigation status of events that have been annotated, if any, and assigned to users for follow-up.



## Customer Tab

The Customer tab contains four 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 of all customers over time when events are generated for these customers.
- **Number of Events per Attacker Address List:** Shows the aggregated event count for events from each attacker address.
- **Event Counts List:** Shows the total number of events and the numbers different attacking and targeted addresses.





## Chapter 6

# Interactive Discovery Partial Project

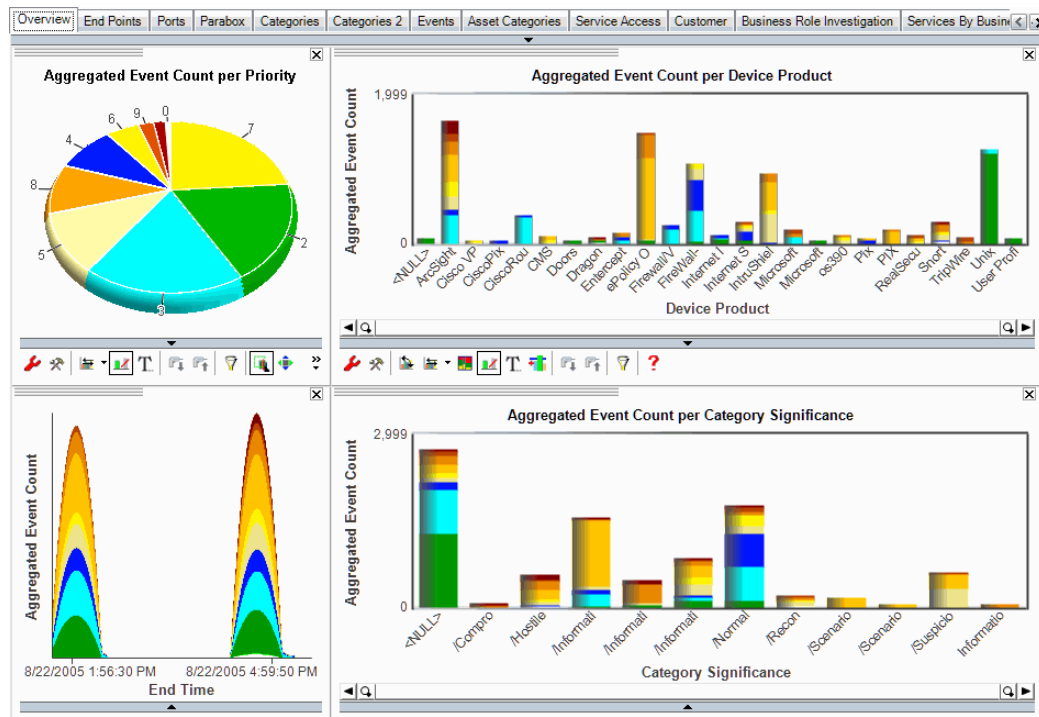
The tabs provide multiple unique views of the data contained in this data set. Use the “partial” reports provided in the package (the ARB file) to generate the data appropriate for the partial project.

The partial 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.

## Overview Tab

The Overview tab contains four charts.

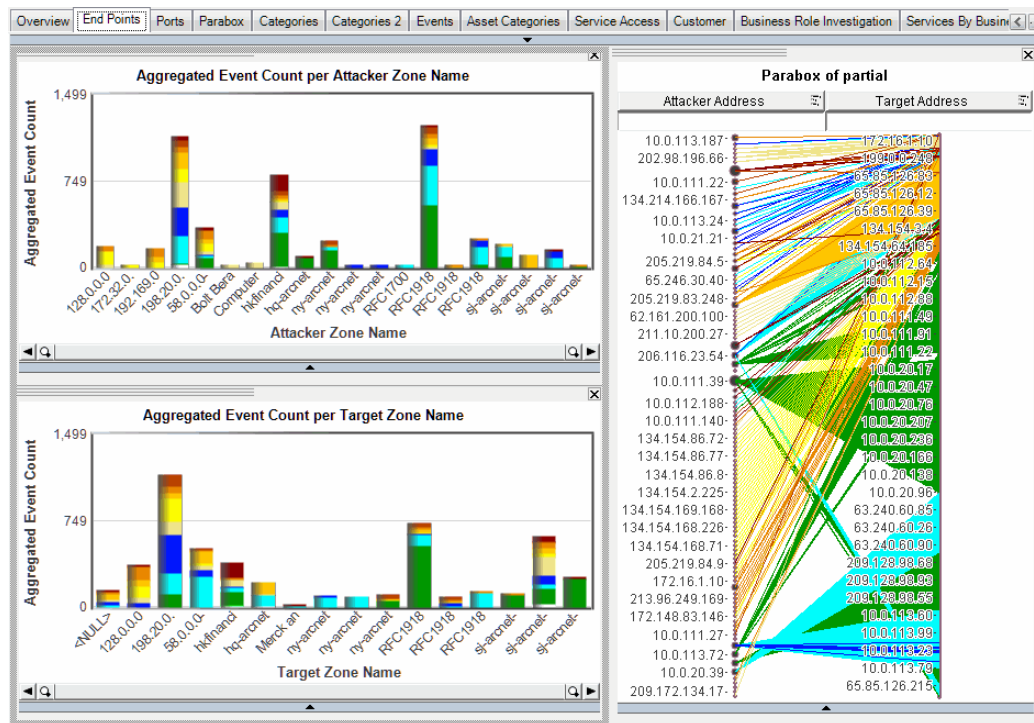
- **Aggregated Event Count per Priority:** shows a pie chart of the number of events of each priority as determined by the ArcSight priority formula.
- **Aggregated Event Count per Device Product:** shows the number of aggregated events by device product (ArcSight, MS Windows, Unix, and so on).
- **Aggregated 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.

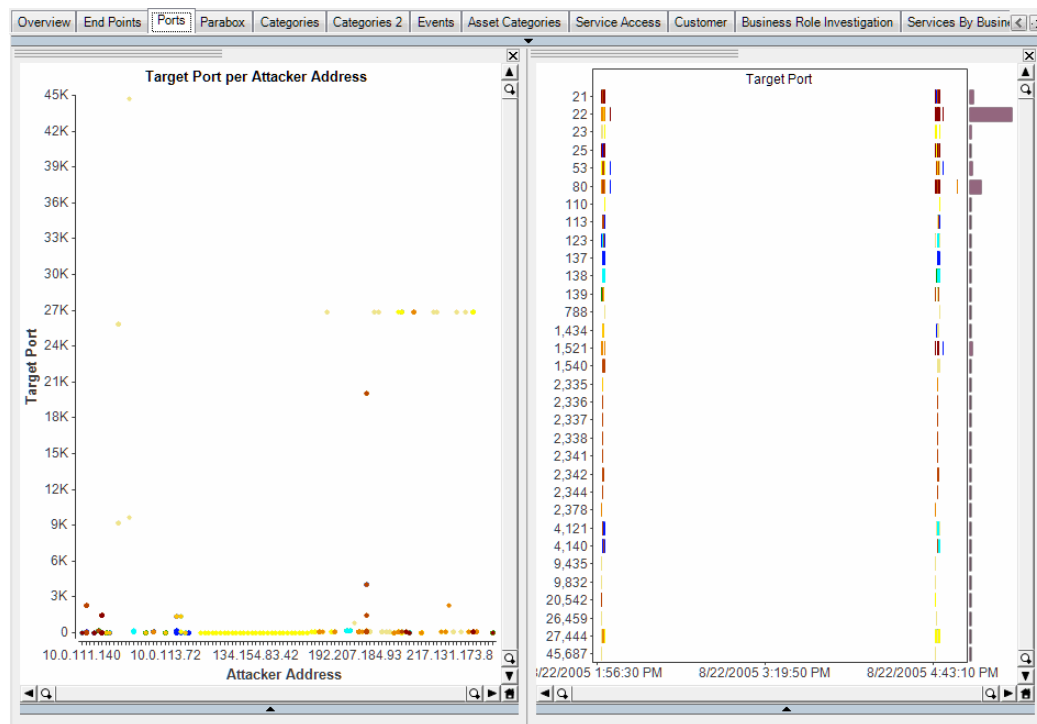


## Ports Tab

The Ports tab contains two charts:

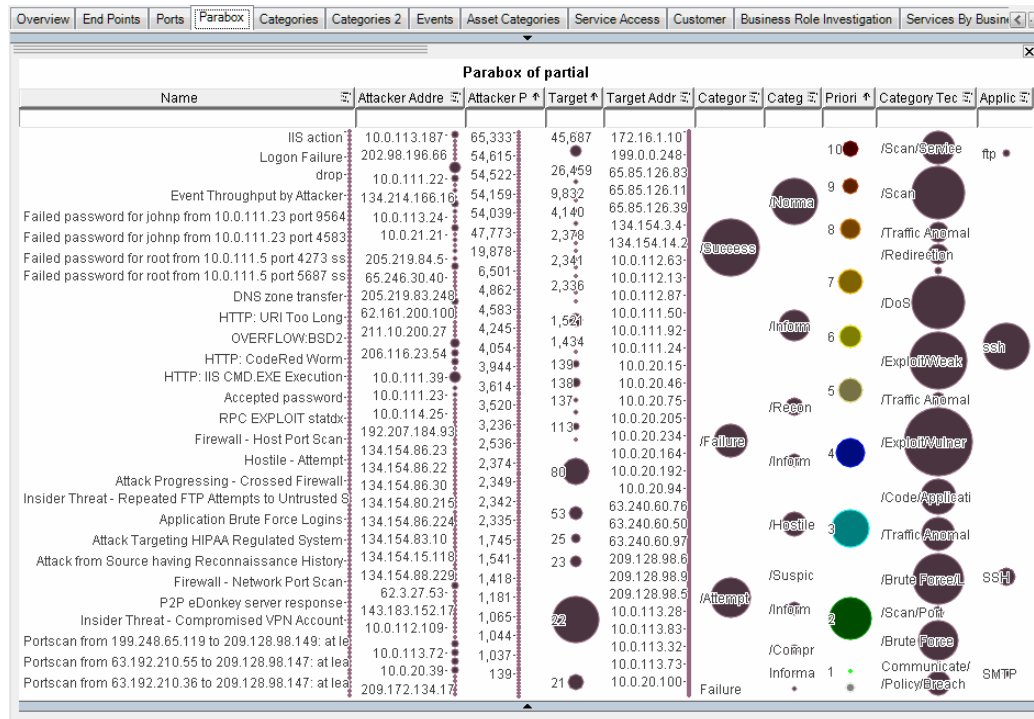
- **Target Ports per Attacker Address:** This scatter plot chart shows target ports on the left, attacker addresses on the bottom. In this chart, you can look for conditions such as services running on ports above 1024, which could warrant investigation, or you can exclude them from the view if they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



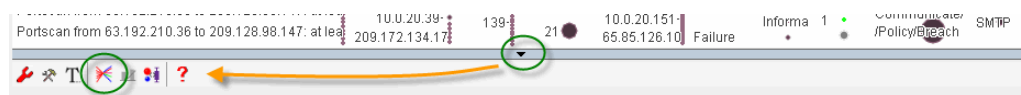
## Parabox Tab

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.



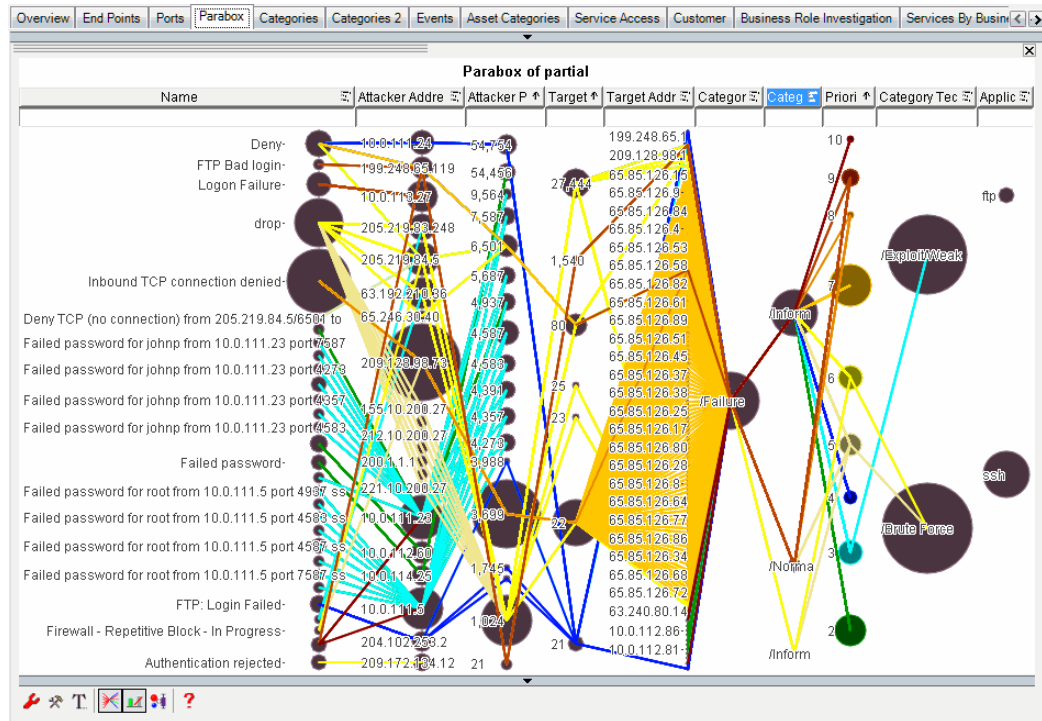
To investigate in the parabox:

- 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 **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:

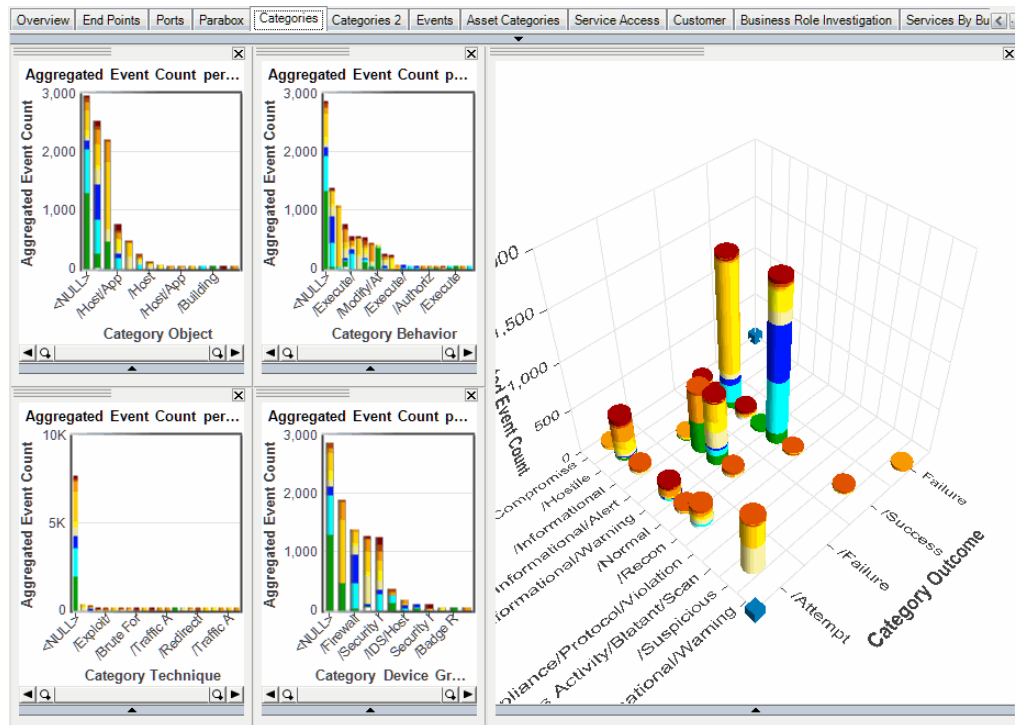


## Categories Tab

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.

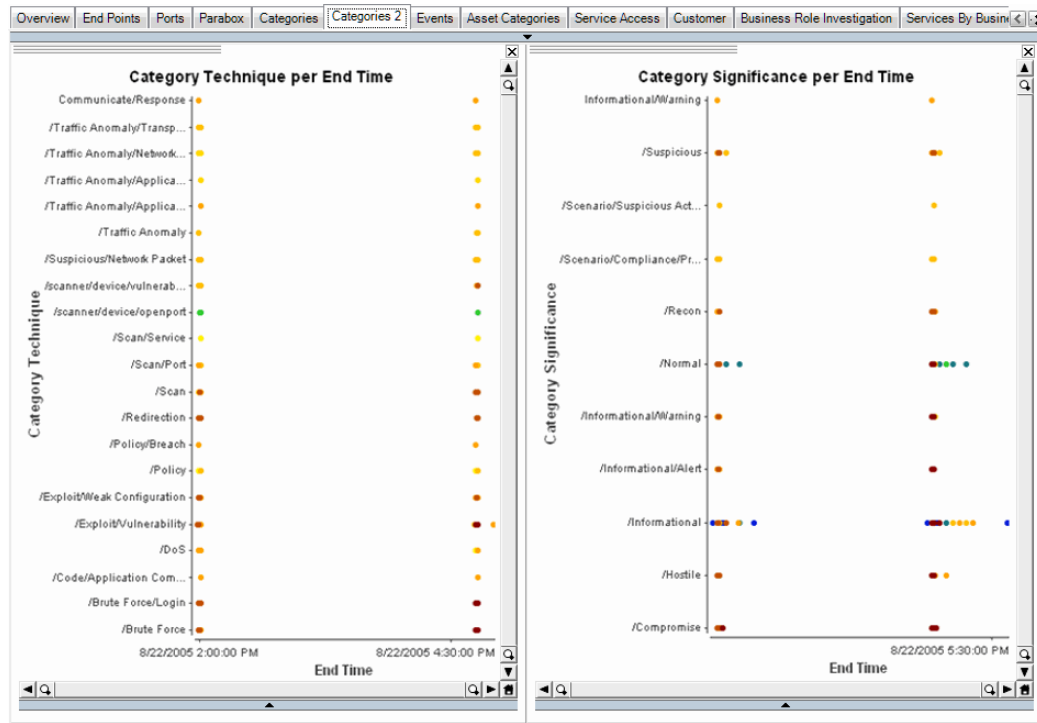
- **Aggregated Event Count per Category Object:** For each category of objects (host, application, service, and so on), it shows the number of aggregated events.
- **Aggregated Event Count per Category Behavior:** For each category of behaviors (access, add, delete, execute, and so on), it shows the 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

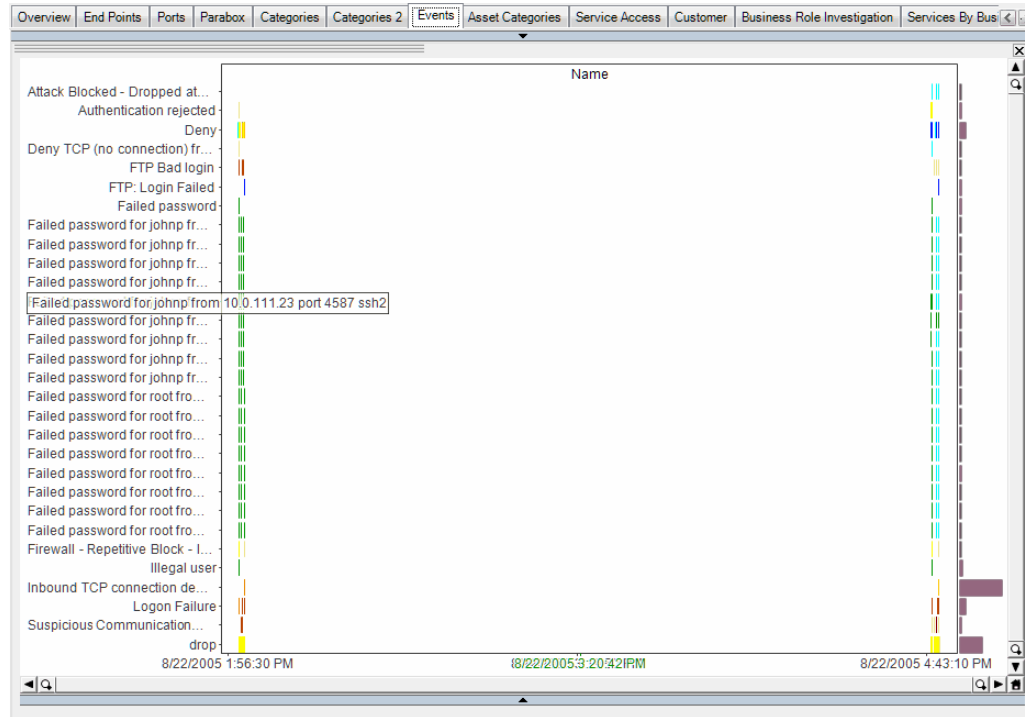
The Categories 2 tab contains two more charts:

- **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.

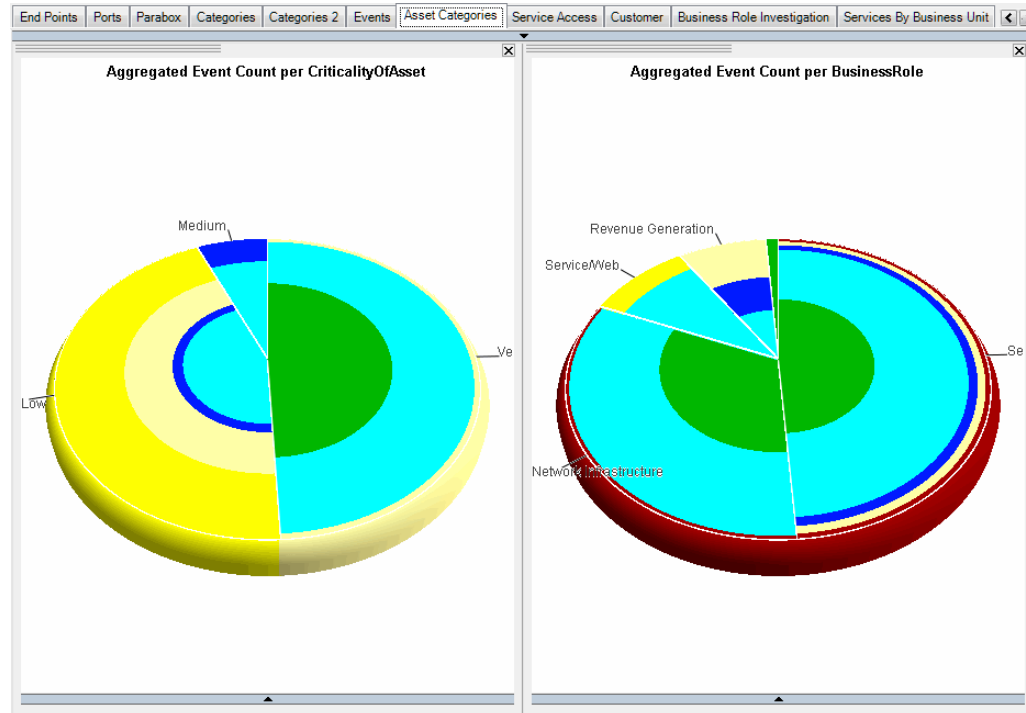


## Asset Categories Tab

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.

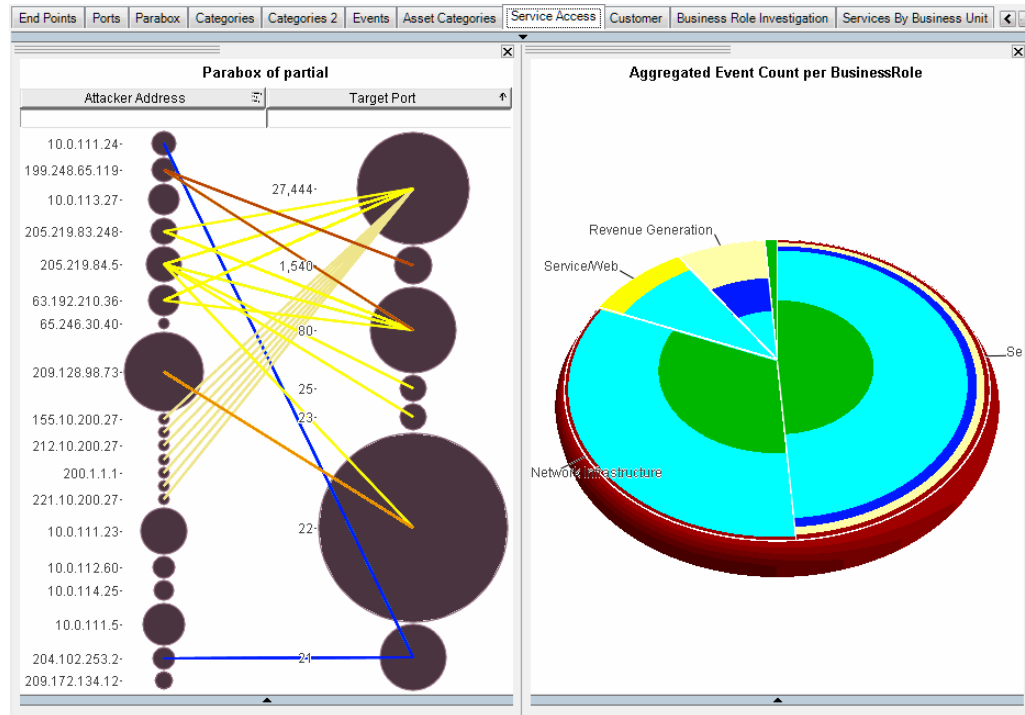
Mouse over the various sections for a description of their contents.



## 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.



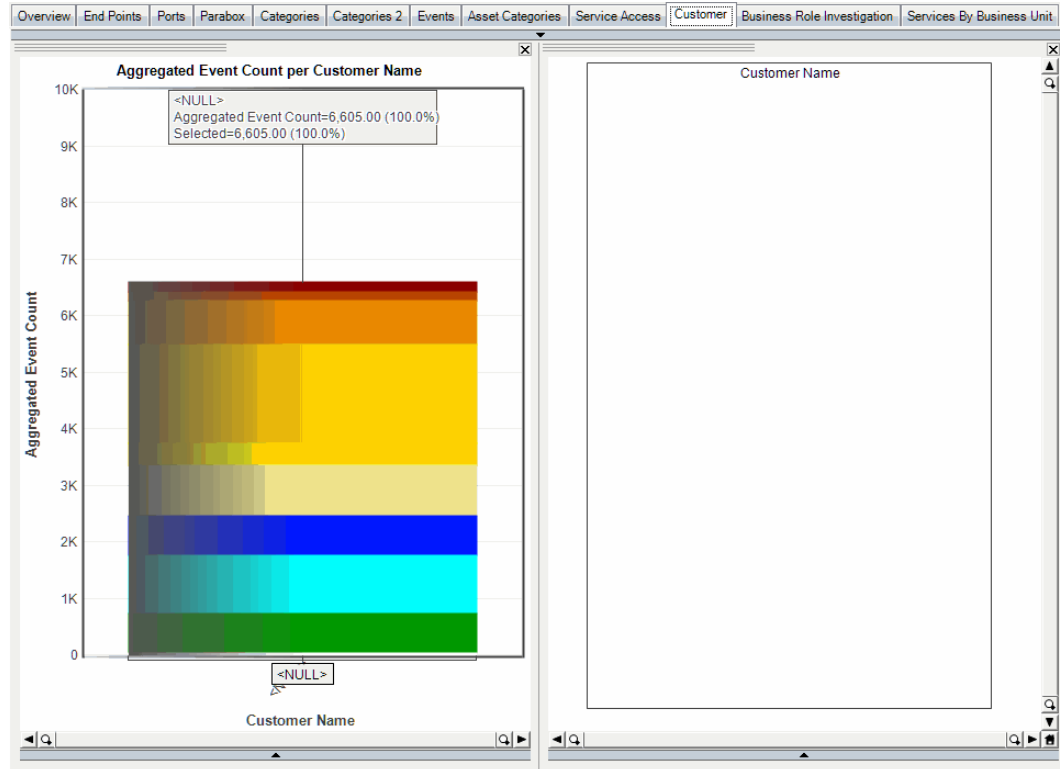
You can select target ports of interest, then see the business role of the events involved in the chart. For example, if you click the large port 22 bubble, then click the Exclude Unselected button, you see the attacker addresses and the business roles of the machines involved.

## 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.



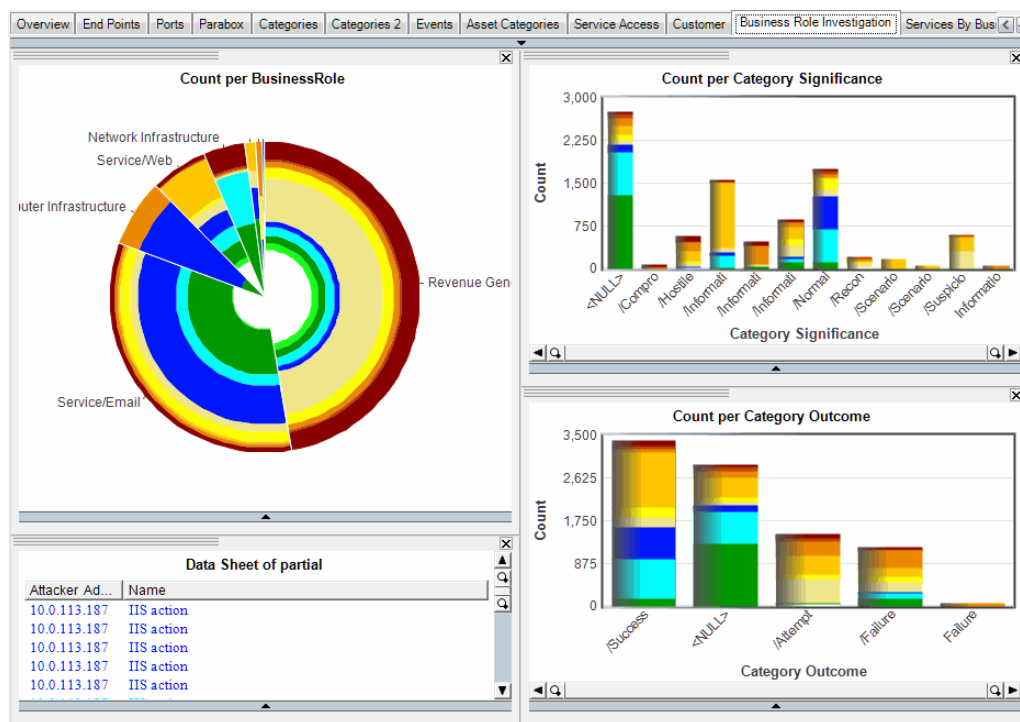
## Business Role Investigation Tab

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.

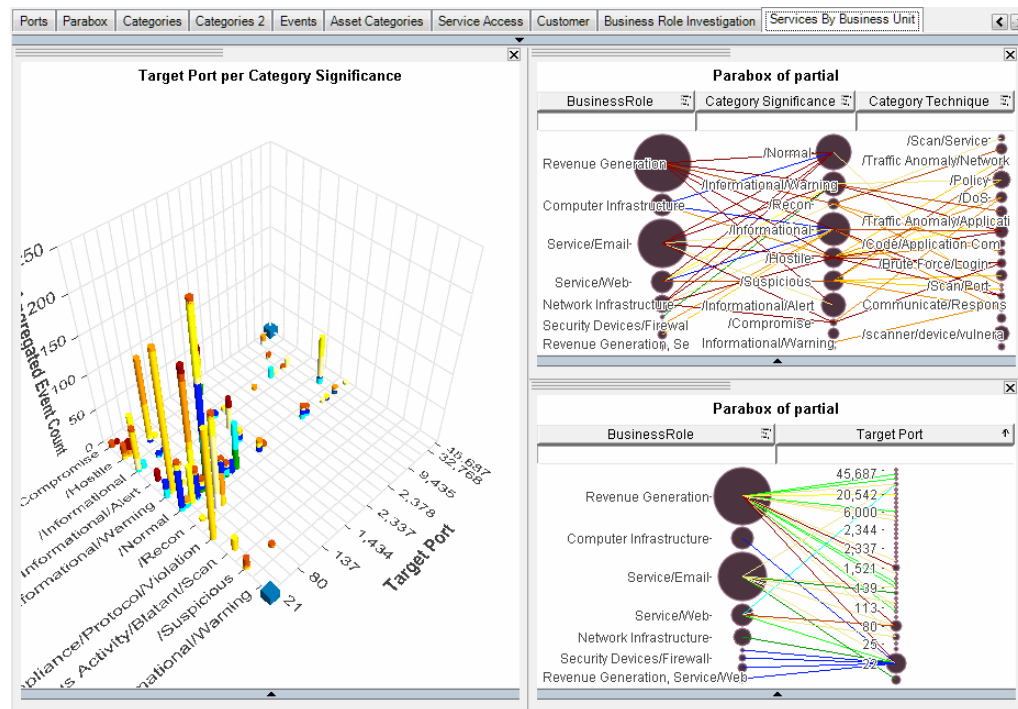




## Services by Business Unit Tab

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.





# Interactive Discovery Use Cases

---

The two data files ArcSight Interactive Discovery ships with, `full.csv` and `partial.csv`, 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” on page 51](#)
- [“Use Case 1: Explore Security Data on Port 23” on page 53](#)
- [“Use Case 2: Analyze Security Data from the Firewall” on page 54](#)
- [“Use Case 3: Export Bookmarks to a Presentation” on page 59](#)

## 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 bookmarks into a summary spreadsheet for the CSO. For the manager of security operations, you can export bookmarked Interactive Discovery data into a Microsoft Word document so you can build a more detailed report.

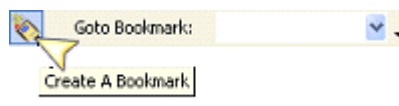
## About Bookmarks

Bookmarks are Interactive Discovery's way of taking a snapshot of the selection and color states you make on a page during your analysis. Once you have selected the conditions and color states you want to communicate, you can add a bookmark. This saves the snapshot in a format that can be exported to PowerPoint or Word.

Bookmarks are saved outside the project, but are erased when a new data set is imported.

To create a bookmark:

- 1 When you have selected the and color states you wish to communicate, click the bookmark icon in the toolbar:










- 2 In the New Bookmark dialog, enter a name for the bookmark and click **OK**.

For complete instructions about how to work with bookmarks, see the Interactive Discovery online Help topic “Bookmark View” in the “Using views” topic.

## 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.
 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.

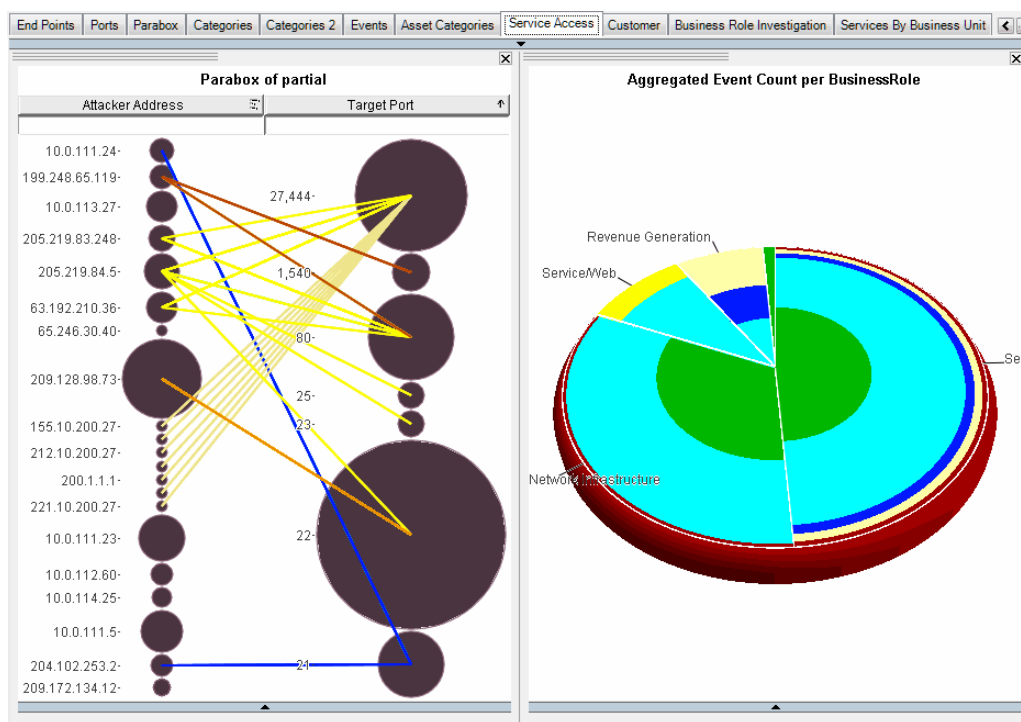
## Use Case 1: Explore Security Data on Port 23

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 partial 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:

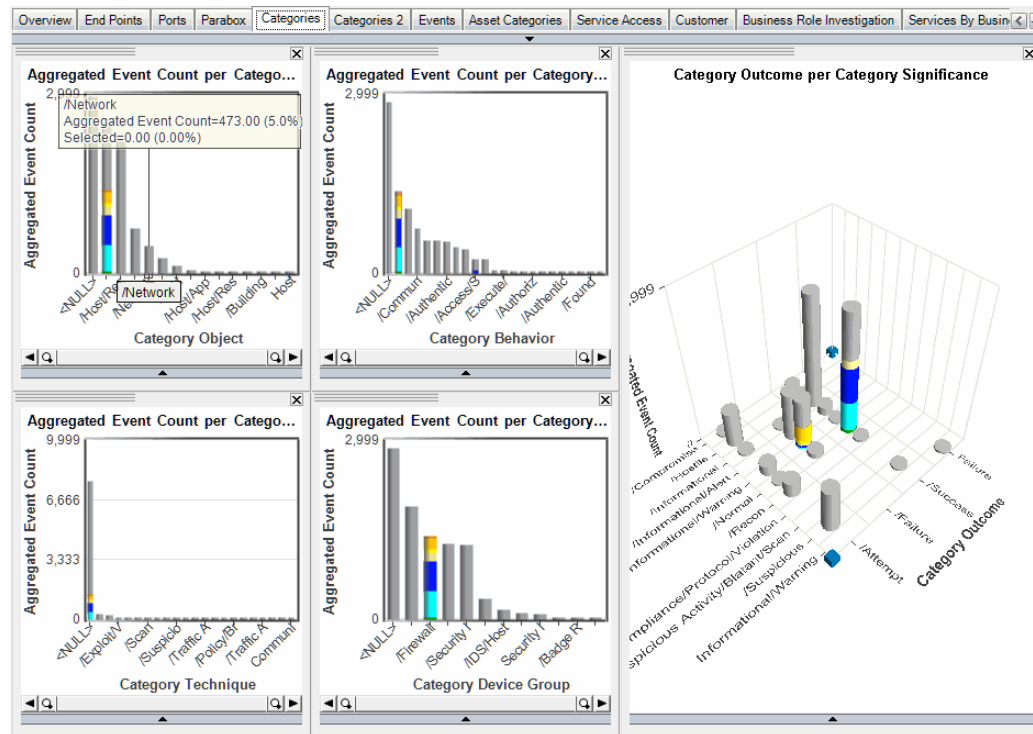
- Which systems reported the events (Over, Parabox)
- What systems that traffic targets (End Points, Parabox, Service Access)
- The business unit of the systems involved (Services by Business Unit, Business Role investigation)
- The category outcome of the events, such as success, failure, attempt (Categories,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



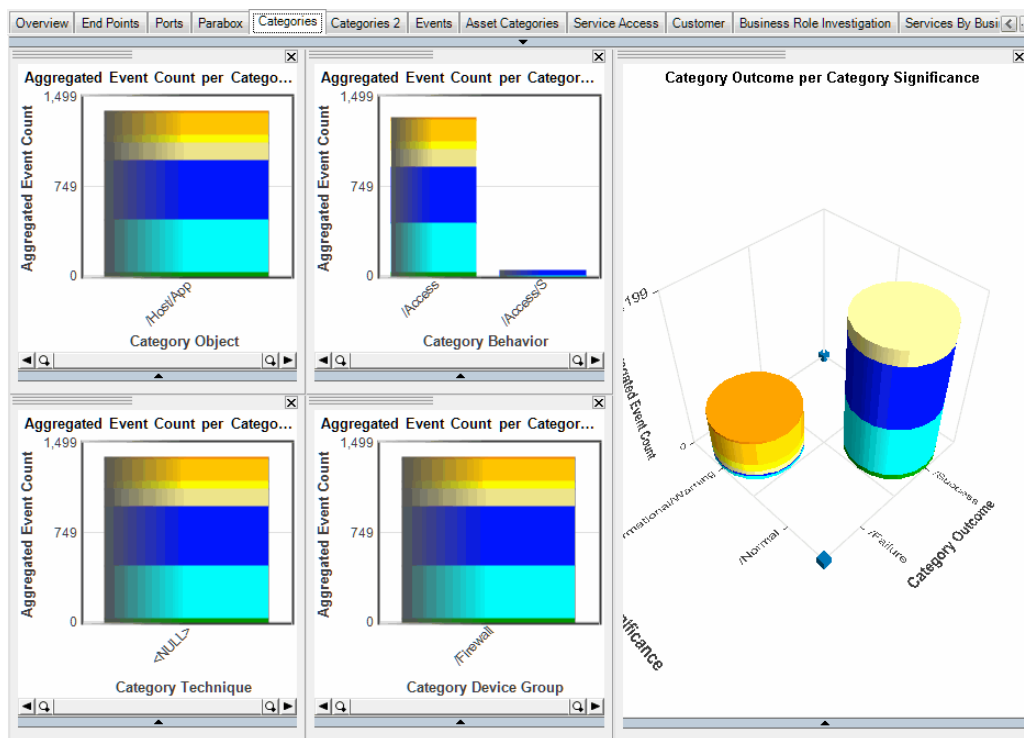
## Use Case 2: Analyze Security Data from the Firewall

One common security scenario to explore is firewall activity in a partial project.

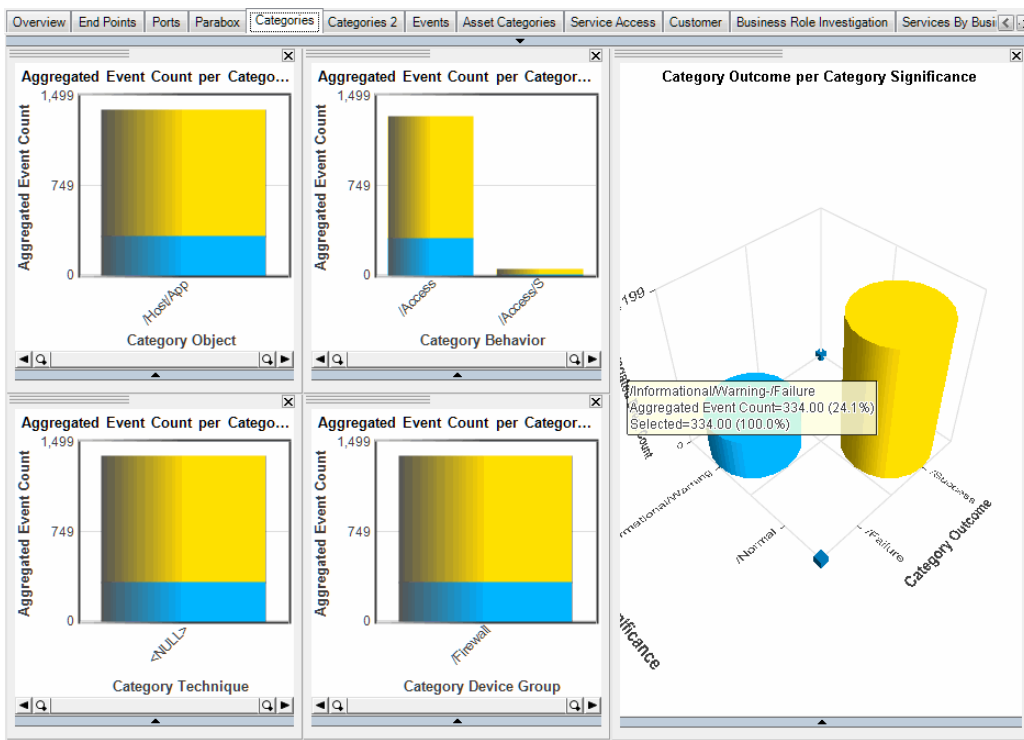
- 1 On the Categories tab, go to Aggregated Event Count per Category Device Group.
- 2 Click on the Firewall bar of the bar chart to select all firewall events.



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

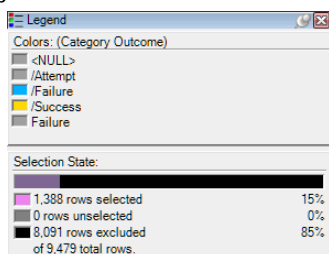


- 4 To see which events succeeded in passing packets through the firewall and which events failed (were blocked by the firewall), go to the Color By drop-down menu in the toolbar and select Category Outcome.

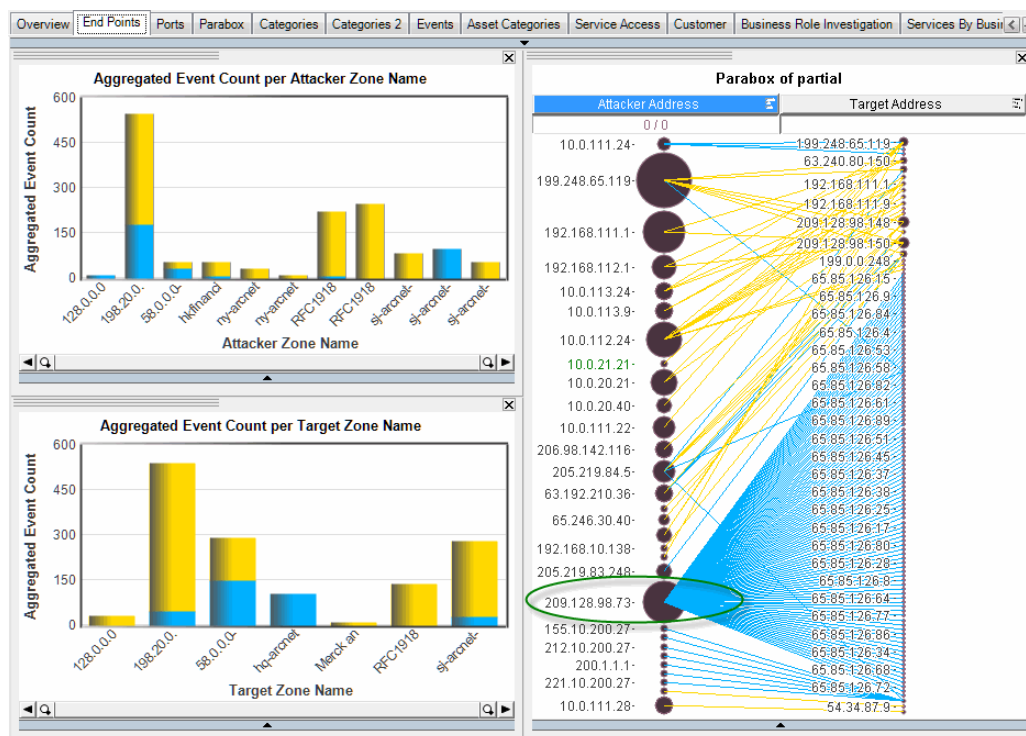


- 5 Create a bookmark of this page. To set a bookmark, click the bookmark toolbar button (🔖) and enter a name, such as *Firewall Successes and Failures*.

- 6 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.



- 7 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 machines. A pattern like this indicates potential malicious behavior.



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

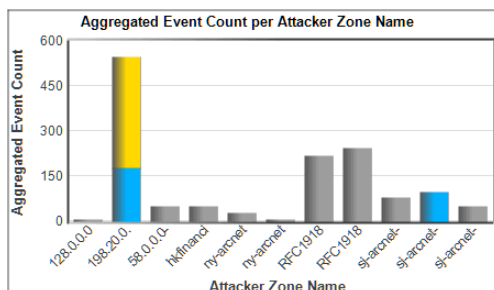
To set a bookmark, click the bookmark toolbar button (🔖) and enter a name, such as *Many connection failures from a single attacker*.

- 8 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

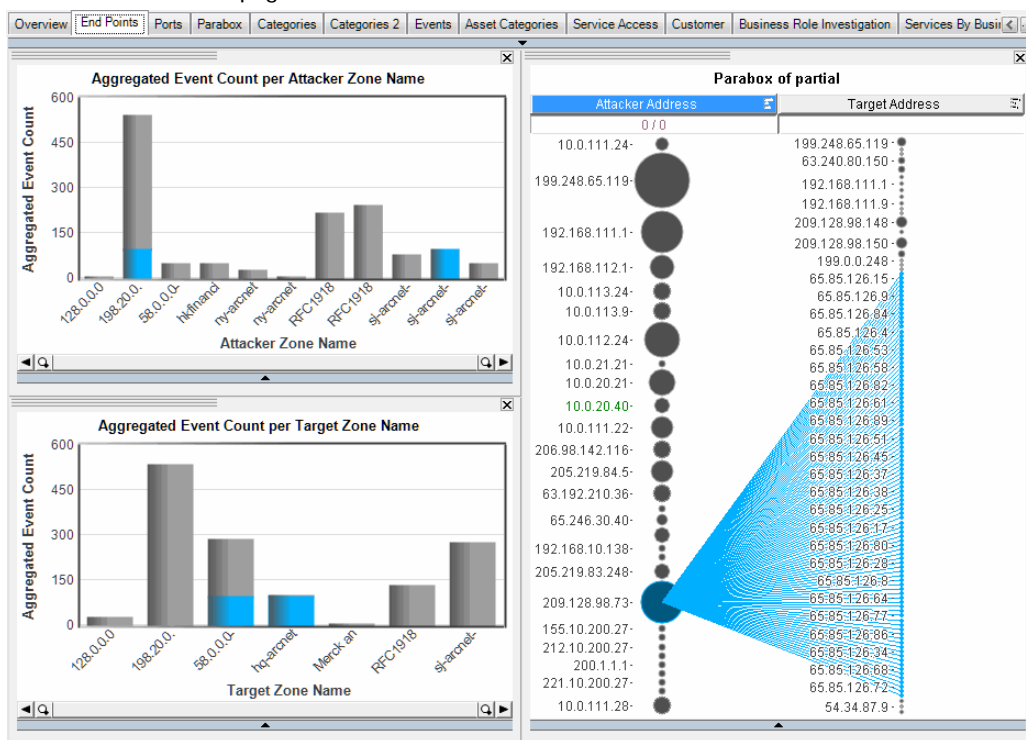


contain blue: 198.20.0.0 - 222.255.255.255 and sj-arcnet-dmz. This shows which zones are involved in the failed connection attempts.

- 9 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.

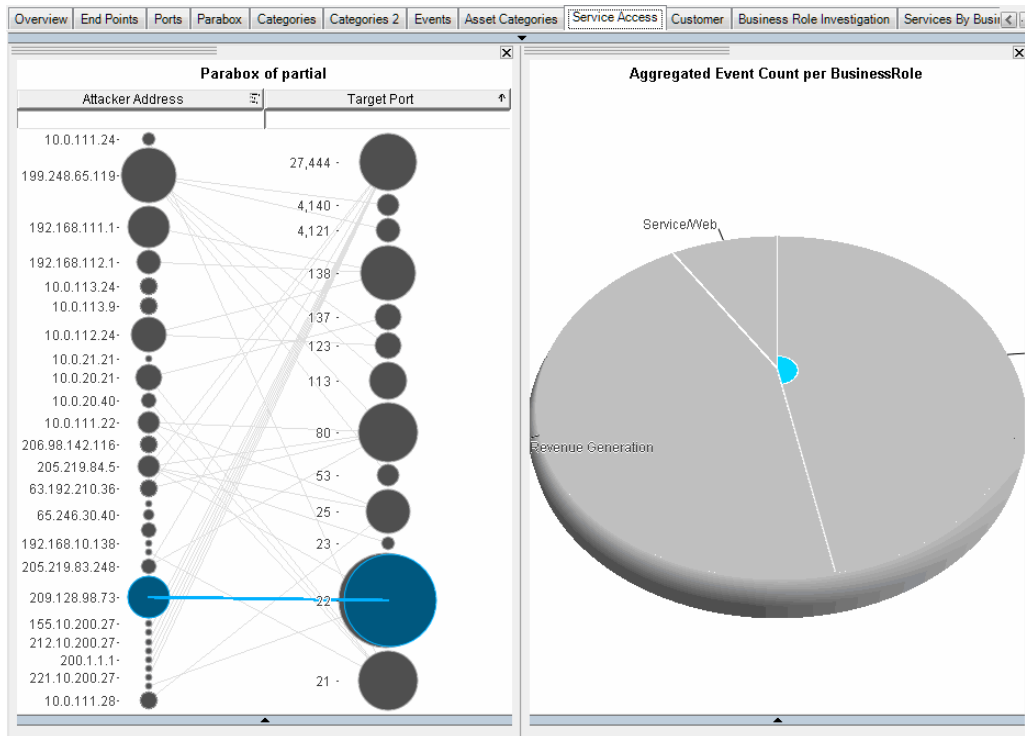



- 10 Next, investigate which ports the malicious attacker address connected to. Click the malicious attacker node to select just that activity. This highlights these connections in the other pages.



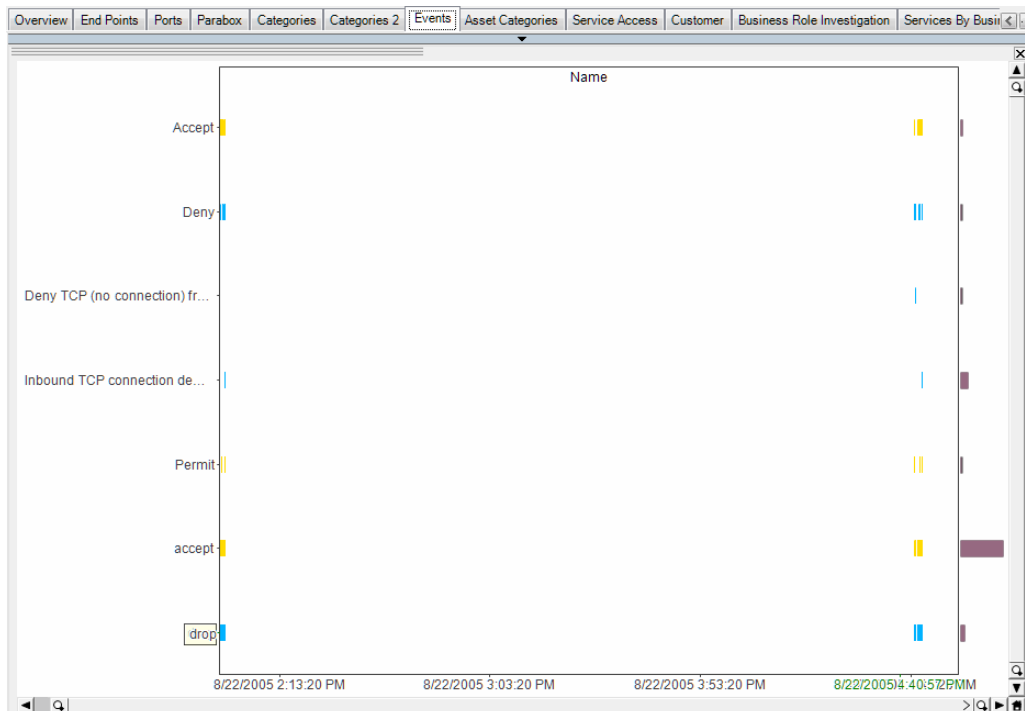
- 11 Click the Service Access tab. This shows the ports to which the malicious attacker has connected. According to the data, it was using only one port on different machines. This indicates that it could be a worm, which probes machines for the same port. On the other hand, if the target port that is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

See below: The attacker was probing different machines for port 22. Bookmark this .

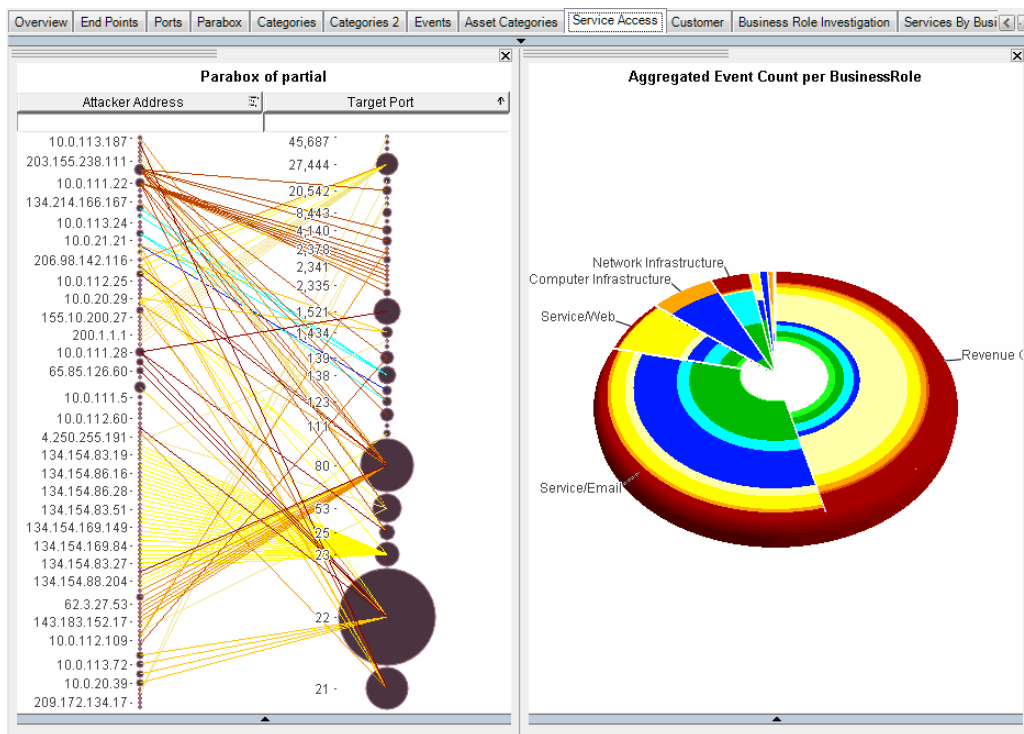


To set a bookmark, click the bookmark toolbar button (  ) and enter a name, such as *Attack Targets Port 22*.

- 12** 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.



- 13** 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.



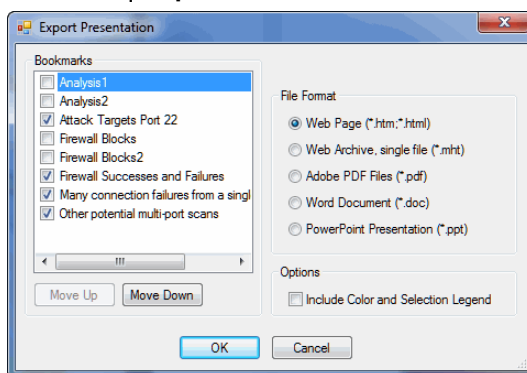
Set another bookmark. To set a bookmark, click the bookmark toolbar button (🔖) and enter a name, such as *Other potential multi-port scans*.

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

## Use Case 3: Export Bookmarks to a Presentation

Once you have set some bookmarks, you can re-order them before exporting them to a PowerPoint or Word file.

- 1** Go to **File | Export Presentation**.



- 2 In the Export Presentation dialog box at the Bookmarks section, the bookmarks you created are listed in alphabetical order. Use the check boxes to select which bookmarks you want to export. To re-order a bookmark, click the bookmark name (not the checkbox) and use the **Move Up/Move Down** buttons.
- 3 In the File Format section, choose an output file format (html, web archive, Adobe PDF, Word, PowerPoint).
- 4 In the Options section, choose **Include Color and Selection Legend**. This clearly communicates what the colors in your snapshot represent.
- 5 In the Destination section, click **Browse**.
- 6 In the **Save As** dialog box, browse to an export location, provide a file name, and click **Save**.
- 7 In the Export Presentation dialog, click **OK**.
- 8 When the presentation is finished, the system displays the message "Presentation saved to the following location..." You can click the link to open the presentation. Click **OK** to close the dialog.




## Appendix A







# Full and Partial Schemas

---

This appendix lists the event fields contained in the [full.csv](#) and [partial.csv](#) files.

All Full Schema fields are listed in the table, below. The fields that are also in the partial schema are indicated by “Yes” in the right-hand column. For a description of the event groups, see *ArcSight 101*, chapter 3, “ArcSight Event Schema.”

Event Group	Event Field	Type	Partial
 Event (root)	Aggregated Event Count	Integer	Yes
	Application Protocol	Text	Yes
	Bytes In	Integer	Yes
	Bytes Out	Integer	Yes
	Correlated Event Count	Integer	Yes
	Customer Name	Text	Yes
	End Time	DateTime	Yes
	Generator Name	Text	
	Manager Receipt Time	DateTime	
	Name	Text	Yes
	Start Time	DateTime	
	Transport Protocol	Text	Yes
	Type	Text	
	Vulnerability Name	Text	Yes
 Agent	Agent Address	Text	
	Agent Host Name	Text	
	Agent Name	Text	
	Agent Receipt Time	DateTime	
	Agent Severity	Text	
	Agent Time Zone	Text	
	Agent Type	Text	
	Agent Version	Text	
	Agent Zone Name	Text	
 Attacker	Attacker Address	Text	Yes
	Attacker Asset Name	Text	
	Attacker DNS Domain	Text	
	Attacker FQDN	Text	
	Attacker Geo Country Code	Text	
	Attacker Geo Country Name	Text	
	Attacker Geo Latitude	Double	Yes
	Attacker Geo Longitude	Double	Yes
	Attacker Host Name	Text	
	Attacker Mac Address	Text	
	Attacker NT Domain	Text	
	Attacker Port	Integer	Yes
	Attacker Process Name	Text	
	Attacker Service Name	Text	
	Attacker Translated Address	Text	

Event Group	Event Field	Type	Partial
 Attacker (Continued)	Attacker Translated Port	Integer	
	Attacker Translated Zone Name	Text	
	Attacker User ID	Text	
	Attacker User Name	Text	
	Attacker User Privileges	Text	
	Attacker Zone Name	Text	Yes
 Category	Category Behavior	Text	Yes
	Category Device Group	Text	Yes
	Category Object	Text	Yes
	Category Outcome	Text	Yes
	Category Significance	Text	Yes
	Category Technique	Text	Yes
 Device	Device Action	Text	Yes
	Device Address	Text	Yes
	Device Direction	Text	
	Device Dns Domain	Text	
	Device Event Category	Text	
	Device Event Class ID	Text	
	Device External ID	Text	
	Device Host Name	Text	
	Device Inbound Interface	Text	
	Device Mac Address	Text	
	Device NT Domain	Text	
	Device Outbound Interface	Text	
	Device Process Name	Text	
	Device Product	Text	Yes
	Device Receipt Time	DateTime	
	Device Severity	Integer	
	Device Time Zone	Text	
	Device Vendor	Text	Yes
	Device Version	Text	
	Device Zone Name	Text	Yes
	Device Custom Number 1	Integer	
	Device Custom Number 2	Integer	
	Device Custom Number 3	Integer	
	Device Custom String 1	Text	
	Device Custom String 2	Text	
	Device Custom String 3	Text	
	Device Custom String 4	Text	
	Device Custom String 5	Text	
	Device Custom String 6	Text	
 Event Annotate	Annotation Comment	Text	
	Annotation Flags	Text	
	Annotation Modification Time	DateTime	
	Annotation Modified By	Text	
	Annotation Stage	Text	
	Annotation User	Text	
 File	File ID	Text	
	File Name	Text	Yes
	File Path	Text	
	File Permission	Text	
	File Type	Text	
 Old File	Old File Name	Text	

Event Group	Event Field	Type	Partial
 Request	Request Client Application	Text	
	Request Context	Text	
	Request Cookies	Text	
	Request Method	Text	
	Request Protocol	Text	
	Request URL	Text	Yes
	Request URL Authority	Text	
	Request URL File Name	Text	
	Request URL Host	Text	
	Request URL Port	Text	
	Request URL Query	Text	
 Target	Target Address	Text	Yes
	Target Asset Name	Text	
	Target DNS Domain	Text	
	Target FQDN	Text	
	Target Geo Country Code	Text	
	Target Geo Country Name	Text	
	Target Geo Latitude	Double	Yes
	Target Geo Longitude	Double	Yes
	Target Host Name	Text	
	Target Mac Address	Text	
	Target NT Domain	Text	
	Target Port	Integer	Yes
	Target Process Name	Text	
	Target Service Name	Text	
	Target Translated Address	Text	
	Target Translated Port	Integer	
	Target Translated Zone Name	Text	
	Target User ID	Text	
	Target User Name	Text	
	Target User Privileges	Text	
	Target Zone Name	Text	Yes
 Threat	Priority	Integer	Yes
	Relevance	Integer	Yes
	Severity	Integer	Yes
	Criticality of Asset	Text	Yes
	Business Role	Text	Yes





# Index

---

## A

- ARB content file 11
- ArcSight support 10
- Asset Categories tab
  - full 32
  - partial 45
- Attacker Details tab 24
- Attacker tab 23
- attackers
  - by country 23
  - by host name 23
  - by port 23
  - by zone name 23
  - to target addresses 27
- Attacks filter 14
- audience 6
- Authentication and Authorization filter 14

## B

- behavior
  - events per 28
- bookmark 51
- browser 9
- business role
  - by target port 33
  - events by 32
- Business Role Investigation tab 48
- Business Unit tab 33

## C

- categories
  - events per behavior 28
  - events per device 28
  - events per object 28
  - events per outcome 29
  - events per significance 29
- Categories (continued) tab 29
- Categories 2 tab 43
- Categories tab
  - full 28
  - partial 42
- Category by Time tab 31
- Category Significance tab 30
- colors 19
- CPU 7
- critical servers attacks 14
- criticality 21
- CSV
  - generation 15

- Customer tab
  - partial 35, 47

## D

- data point details 19
- device
  - events per 28
- display resolution 10
- download 10

## E

- End Points tab 38
- Event List tab 21
- events
  - by asset criticality 32
  - by attacker address 22
  - by business role 32
  - by customer name 35
  - by device product 37
  - by end time 22
  - by name and time 22
  - by priority 22
  - by stage 34
  - by target host 25
  - by target port 25
  - by user 34
  - stage
    - annotation stage, user 34
- events per port 30
- Events tab
  - full 27
  - partial 44
- exclude unselected 52

## F

- filters 12
  - full project 21
- full schema 21

## G

- graphics display 10

## H

- hardware 10
- help, in AID 19
- HP support 10

## I

INI file 16  
Intrusion Detection Systems filter 14

## J

Job Frequency window 18

## L

Locate Missing Data File dialog 17

## O

operating system 9  
Operating System filter 14  
outcome  
    events per 29  
overview  
    data 13  
    installation 7  
    product 5  
Overview tab  
    full 22  
    partial 37

## P

package, import 11  
Parabox tab 40  
partial schema 37  
performance 10  
Ports tab 39  
project, open 16

## R

RAM 7  
registry 10  
reports 12  
    building 16  
requirements 9

## S

schedule report 17  
schema 21  
selecting elements 52  
Service Access tab 46  
Services by Business Unit tab 49  
setup.exe 10  
significance 30  
    and technique 33  
    by time 31  
    events per 29  
    per outcome 30

## T

Target Details tab 26  
Target tab 25  
targets  
    by business role 33  
    by zone 25  
    of attacker addresses 27  
    port by significance 30  
technique  
    and significance 33  
    events per 29

## U

uninstall  
    previous version 10  
    procedure 12

## V

video RAM 10

## W

Workflow tab 34

## Z

ZIP file extraction 10, 11