CrossTec Corporation

Evaluator's Guide

Activeworx Security Center 3.0

Activeworx Security Center 3.0 Evaluator's Guide

PREPARED BY ALBERT CABALLERO

CONTRIBUTIONS BY GARY CONKLE AND JEFF DELL

© CrossTec Corporation
500 NE Spanish River Blvd. • Suite 201
Phone 800.675.0729 • Fax 561.391.5820
www.CrossTecCorp.com

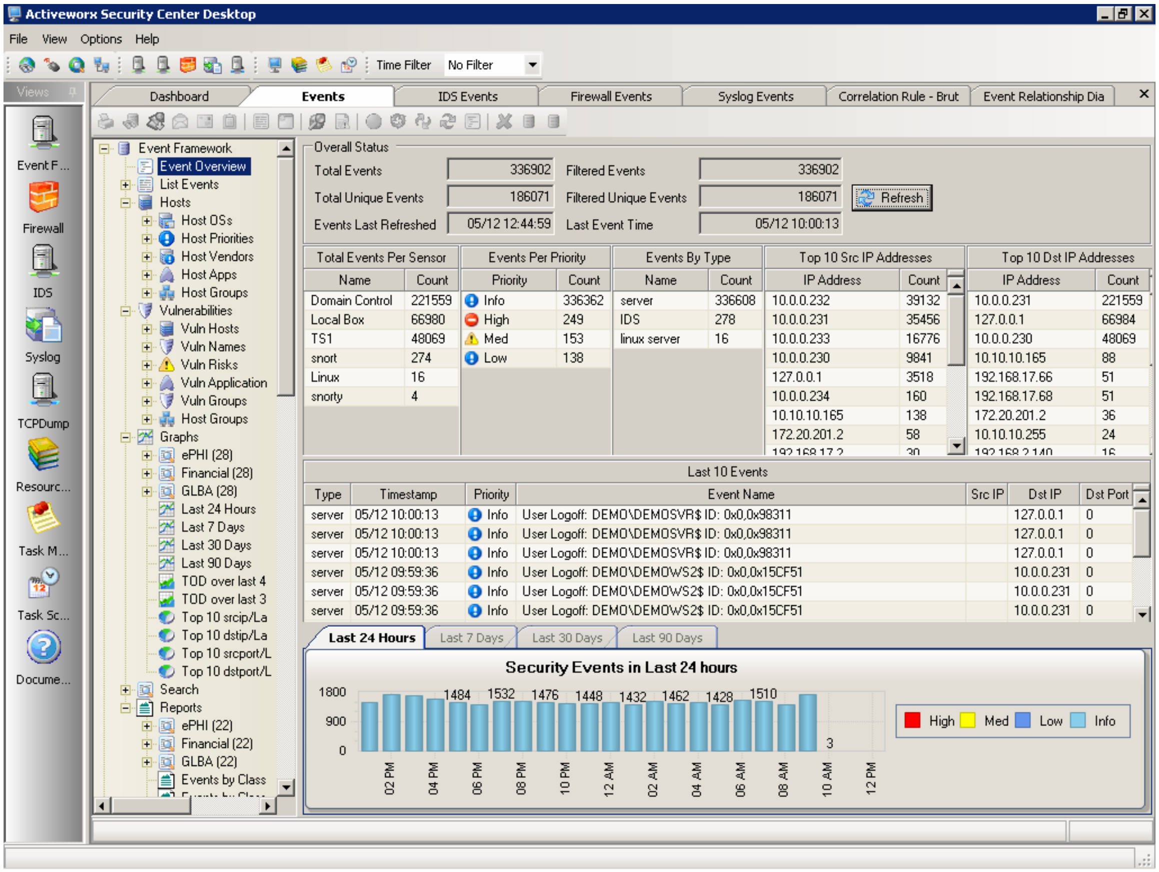
Table of Contents

Introduction

Abstract

As enterprise networks and security log data grow, the need for stable and affordable Security Information Management (SIM) is steadily increasing. A greater percentage of IT budgets now go to security hardware and software more than ever before, as companies deploy an army of firewalls, intrusion detection and prevention systems (IDS/IPS), email gateways, and VPNs; as well as a combination of other defenses primarily designed to help mitigate the actions of malicious users and to meet regulatory compliance. Having success in defending your network isn't just a matter of increasing firepower - it also depends on effective correlation between security events. Activeworx Security Center (ASC) is an application-based SIM tool that is scalable enough to meet the requirements of the most complex security infrastructures, as well as modular enough to be a low-cost solution for the smaller shops that may only run a few Windows servers, a firewall, and/or an Intrusion Detection System (IDS). What's more, ASC can help make it possible to implement otherwise prohibitive defensive solutions such as IDS, because of the amount of time it can save in log analysis and event correlation.

Throughout this guide we will explain how to best utilize ASC as a SIM solution to help build network intelligence, view security events and correlate them among different devices, as well as automate compliance reports and email or Syslog alerts. Below is a screenshot of the ASC Event Framework database – Event Overview screen.



Overall Status

Total Events	336902	Filtered Events	336902
Total Unique Events	186071	Filtered Unique Events	186071
Events Last Refreshed	05/12 12:44:59	Last Event Time	05/12 10:00:13

Total Events Per Sensor		Events Per Priority		Events By Type		Top 10 Src IP Addresses		Top 10 Dst IP Addresses	
Name	Count	Priority	Count	Name	Count	IP Address	Count	IP Address	Count
Domain Control	221559	Info	336362	server	336608	10.0.0.232	39132	10.0.0.231	221559
Local Box	66980	High	249	IDS	278	10.0.0.231	35456	127.0.0.1	66984
TS1	48069	Med	153	linux server	16	10.0.0.233	16776	10.0.0.230	48069
snort	274	Low	138			10.0.0.230	9841	10.10.10.165	88
Linux	16					127.0.0.1	3518	192.168.17.66	51
snorty	4					10.0.0.234	160	192.168.17.68	51
						10.10.10.165	138	172.20.201.2	36
						172.20.201.2	58	10.10.10.255	24
						192.168.17.2	30	192.168.2.140	16

Last 10 Events

Type	Timestamp	Priority	Event Name	Src IP	Dst IP	Dst Port
server	05/12 10:00:13	Info	User Logoff: DEMO\DEMOSVR$ ID: 0x0,0x98311		127.0.0.1	0
server	05/12 10:00:13	Info	User Logoff: DEMO\DEMOSVR$ ID: 0x0,0x98311		127.0.0.1	0
server	05/12 10:00:13	Info	User Logoff: DEMO\DEMOSVR$ ID: 0x0,0x98311		127.0.0.1	0
server	05/12 09:59:36	Info	User Logoff: DEMO\DEMOWS2$ ID: 0x0,0x15CF51		10.0.0.231	0
server	05/12 09:59:36	Info	User Logoff: DEMO\DEMOWS2$ ID: 0x0,0x15CF51		10.0.0.231	0
server	05/12 09:59:36	Info	User Logoff: DEMO\DEMOWS2$ ID: 0x0,0x15CF51		10.0.0.231	0

What is Security Information Management

Security Information and/or Event Management is a growing industry using an innovative class of security management tools that enables security professionals to correlate and analyze data using a common application from a wide variety of sources. SIM is considered a 'Best Practices' approach to managing security events; and with the introduction of SIM, major advances have been made in security information analysis, correlation, and reporting. This has led to many benefits for both IT Security managers as well as auditors. The real challenge for SIM is turning a multitude of disparate security devices and server systems (each with their own logs, data output format, and rule set) into a cohesive defensive arsenal.

To better visualize and understand their security posture, companies are turning to security information management software. SIM software is designed to simplify management of event logs, provide greater visibility of the network, and improve accuracy when responding to incidents on the network. Some SIM systems may even include the added benefit of helping an organization meet regulatory compliance through built-in compliance reporting to improve the response times by using integrated alert features. The goal is not to continuously add more security devices at the problem, but to reduce the amount of time spent reviewing unnecessary logs by intelligently filtering those events of interest that require some type of action by the administrator.

Why Invest in a SIM

Incorrectly managing the risks of protecting your network from malware and adhering to Federal regulations could bring serious consequences, including excessive dollars spent to correct infiltration of network systems and regulatory fines or penalties levied by the Federal Government; not including additional and unexpected expenses for labor, hardware, and insurance.

Designed to identify, analyze, and report on intrusions into the network, Security Information and Event Management (SIM) tools are becoming more common and readily available to organizations of all sizes. Today, both hardware and software solutions exist with the ability to manage the flow of security event data in near real-time. Collecting, organizing, and mining security data on your network makes it possible to run reports on disparate devices and analyze great amounts of data quickly, which are essential elements for in-depth defense and regulatory compliance.

Corporations concerned with protecting critical resources have implemented protective barriers that combine firewalls, IDS, IPS, VPN, anti-virus and other security products; but each product typically acts on its own – producing its own alerts and reports. By aggregating, normalizing, correlating, and prioritizing data from multiple security devices, SIM technologies can convert and prioritize these large volumes of data into intelligent, actionable information, and manage activities from a centralized location.

What to look for in a SIM

SIM tools perform an extremely complex set of functions on a network as the idea is to simplify and automate all of these otherwise complex capabilities. However, some SIM solutions incorporate an enormous amount of features (even within their base products) and this can easily become unwieldy to test and implement on a network of any size. Appliance-based solutions tend to have these common characteristics: A high feature set coupled with high complexity for installation and deployment and a high price tag. Other SIM tools, usually application-based SIM's, tend to have a more modular approach, making it much easier and less expensive to install and configure in a smaller environment, as well as more flexible for the larger security infrastructures. The main categories in which SIM vendors are compared are the following: Ease of installation and use, number of security devices and agents supported, ease of customizing correlation rules and analytics, accurate near real-time display and response to events, and finally cost-effectiveness appropriate to your environment.

About Activeworx Security Center

Activeworx Security Center (ASC) provides a feature rich, user-friendly environment to view security event log files, perform event correlation, and view the overall posture of your security infrastructure. ASC was designed by and for security administrators to provide a common view of all security events in your environment. It allows a user to view, search, graph, diagram, report and correlate between all the different security information that is generated on the network. It does this through an intuitive yet powerful interface that is easier to use than other, much more costly, SIM solutions.

Evaluation Requirements

Please review our Activeworx Quick Install Guide found on your Trial CD image or at http://www.crossteccorp.com/support/resources/ASC_v3_QuickInstall.pdf for evaluation requirements, a quick walkthrough installation, and basic configuration.

NOTE: *Please complete the Quick Install Guide BEFORE running all the exercises in this Evaluator's Guide for the best user experience.*

The ASC Manager

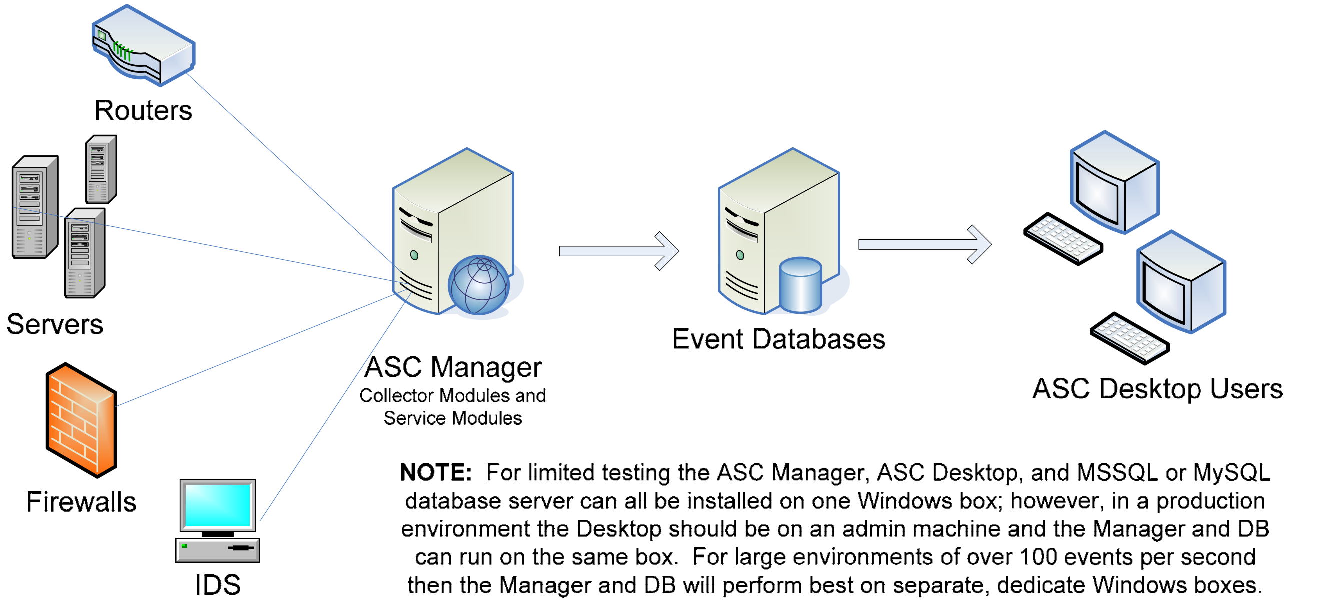
Overview

The Activeworx Security Center Manager is an application that can be installed on one computer or distributed among many within a large network, depending on the functionality of ASC you require. During the Configuration Wizard covered in the Quick Install, you have configured which modules the ASC Manager will be running according to the assets you have selected to monitor. A little later we will take a closer look at placement of the ASC Manager, but for now we can begin with describing the major modules that the ASC Manager can run as a Windows service.

The ASC Manager consists of two different major components: Collector Modules and Service Modules. Typically the ASC Manager needs to be running and collecting events before these events can be viewed within the ASC Desktop, unless you are only managing Snort events in which case no collectors are required. These Collection Modules are what allows an administrator to automate the collection of events. There are several different types of Collector Modules that the ASC Manager can run, the most common of which are the Windows Event Collector, the Network Collector (for Syslog and SNMP), the File Collector, and the Database Collector; we will briefly describe these in the following sections. The Service Modules consist or the Correlation Engine and Scheduling Engine, which are possibly the most important pieces of the ASC solution.

We will briefly describe these as well, and then revisit the placement of the ASC Manager on a couple of typical network environments before opening and viewing events from the ASC Desktop. The Manager and the Desktop are designed to either run on the same machine or be distributed across a WAN, as noted below there is one ASC Manager running many modules however this doesn't always have to be the case. If there is only a need for a single Winlog Collector for example on a specific segment of the LAN then the ASC Manager can be installed and set up to run only that module that is needed.

Below is a diagram of a simple Activeworx implementation for small environments:



NOTE: For limited testing the ASC Manager, ASC Desktop, and MSSQL or MySQL database server can all be installed on one Windows box; however, in a production environment the Desktop should be on an admin machine and the Manager and DB can run on the same box. For large environments of over 100 events per second then the Manager and DB will perform best on separate, dedicate Windows boxes.

Collection Modules

One of the primary roles of the ASC Manager is to collect events from networked systems, normalize all the data into an easy to interpret format, and process all this data based on a set criteria of rules. If it sees events that match its criteria, it imports the events into the appropriate database to be displayed by the ASC Desktop. The ASC Manager usually resides on a separate, dedicated machine that is located close to the devices that it is monitoring. There is no limit to the number of ASC Managers that can work with an ASC solution, and within the ASC Manager resides the Collection Modules that can be licensed to perform different activities.

These modules include:

- **Winlog Collector:** Each Winlog Collector is capable of supporting Windows event collection from up to 255 Windows machines and can generate alerts when certain rules fire. Typically it will open either a Synchronous or an Asynchronous connection to target Windows hosts using WMI and DCOM services that are built into Windows 2000, XP and 2003. This is an active connection from ASC Manager to Windows Host for the pulling of any Windows Event Log.
- **Network Collector:** Used to manage Syslog and SNMP event formats using a service listening on a standard UDP port like 514 for Syslog or 162 for SNMP. This collector can also generate alerts and is typically used to gather events from many disparate network devices such as firewalls, routers and switches, as well as UNIX-based systems. Unlike the Winlog Collector this module is a passive module that sits on the ASC Manager box listening for events so there is no active outbound connection with the Network Collector.
- **Database Collector:** The DB collector is used for moving detailed information from an Activeworx database or a third-party database into the Activeworx Event Framework database. It can also be used for running events through the Correlation Engine. The DB Collector does not generate alerts on its own, only when used in conjunction with a Correlation Engine is it used in this way. This collection module copies events from MySQL and Microsoft databases to bring events into an ASC defined database using native database protocols.
- **File Collector:** Used to load flat files into ASC such as with Windows IIS, Windows XP Firewall or other systems that log to flat files on the system drive. This collection module imports events from flat or XML files by copying files via FTP, SFTP and/or File Copy on a scheduled interval into the processing engine but does not generate alerts on its own.

NOTE: There are other vendor specific supported collectors as well, such as the Cisco IDS Collector and the Checkpoint Collector, which can also be used to pull events using vendor-specific protocols.

Service Modules

The Correlation Engine, new with version 3, allows for active monitoring of network events, trend analysis and alert generation, regardless of the collectors being used. This is a rules based engine which uses a graphical means to build correlation rules and automates alerts over e-mail and Syslog. We will spend a large section towards the end of this guide covering Event Correlation.

The Scheduling Engine is designed to automate all of your administrative tasks (copy, delete, archive, reports) and provide reports distribution (by e-mail, web, etc...) to anyone you wish. This feature is one of the most important in meeting compliance, and reporting to upper management an accurate view of the events that are happening on a daily basis in the organization.

ASC Design

ASC Manager Placement:

ASC Managers should be placed where it is best located for the modules that are running on the Manager, according to the types of devices you need to retrieve events. If a Manager has a Windows Collector that is monitoring a server farm, it should be placed near the servers to reduce network traffic and increase performance. If the server farm generates a lot of events, you might want to consider placing an event database on or near the ASC Manager to allow the Manager to dump the events into a database that is local, as opposed to sending a large amount of events (over a slow WAN link for example). When both the Manager and an event database are located at a remote site, ASC Desktop can be set up to traverse the WAN link and connect to the remote database for viewing events. Whenever possible, ASC Managers should not monitor hosts over a WAN link for events. If the link goes down or a denial of service attack occurs, you could lose events - creating an integrity issue within your audit logs. It is best to place an ASC Manager at each location whenever possible and monitor to a local event database for optimum performance. The Database collector or the scheduling engine could then be used to centralize all events from remote locations to a central operations center.

Database Selection:

ASC is extremely flexible in the way it stores information because you are not bound to a single event database or type. Event databases can be placed at different physical locations or on the same database server for a centralized repository.

There are three types of event databases and each one is tuned to get the best performance it can out of the database server. The three types are:

- **The Firewall database:** A fast streamlined database that stores information about a firewall event in a minimal size record for each event. This should only be used for firewall traffic.
- **The IDS database:** A database that has the ability to store all information for a packet that triggered an IDS event. This database is 100% compatible with Snort's event database.
- **The Activeworx Event Framework (AEF) database:** Used to store information from virtually any type of device on your network. This database not only stores security events - it also stores vulnerability and host information. AEF database is the database of choice for centralizing all events into a common view.

Event Storage:

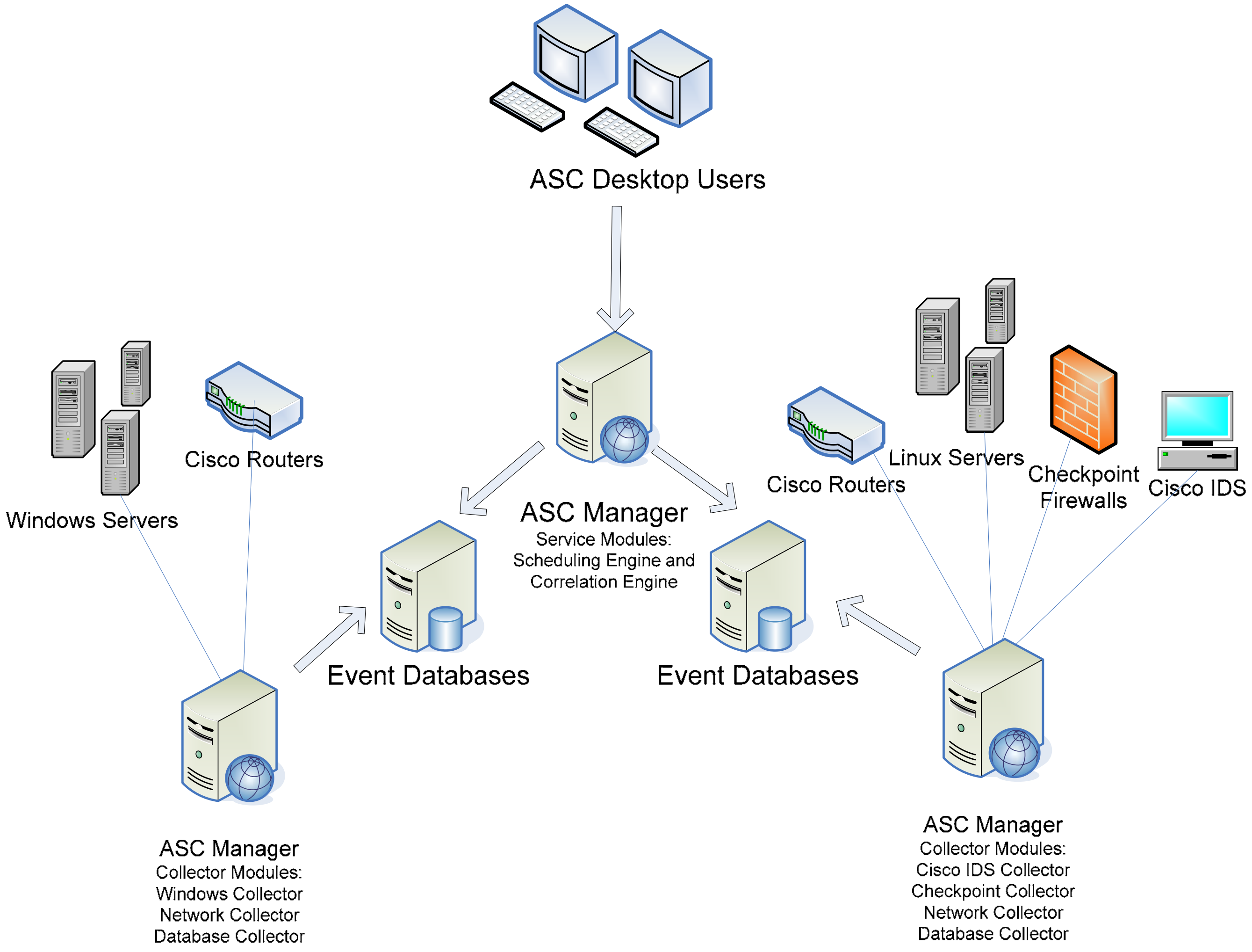
Understanding and selecting event storage can be a difficult task. You will need to look at your environment and understand a few things:

1. How many events per second do you generate on your network?
2. Of those events, how many do you want to store?
3. How long are you required to store events?
4. Do you want to centralize all of you events, keep them in each department, or a combination of both?

These are important questions and will help you spec out the number of event databases and the hardware for event storage. If you are receiving 100 events per second sustained, you will be logging over 8.6 million events per day. The storage space for this many events won't be a concern as much as the processing power, available memory, and the speed of the hard drives on the database servers. If you store the events for a month, it is highly advisable to plan accordingly as this will be nearly 26 millions events per month!

One of the nice things about ASC is that you have full control of the event databases in operation. If you feel that your event database is getting a little slow, you have the ability to move events at scheduled intervals to an archive database. This database can be online all the time to store older events and to run reports on older/archived data if necessary. You also have the ability to store events in event databases that are close to the Manager (such as a remote location or department), then simply use the Database Collector or the Scheduling Engine to centralize all events or only events of interest.

Below is a diagram of a distributed Activeworx implementation:

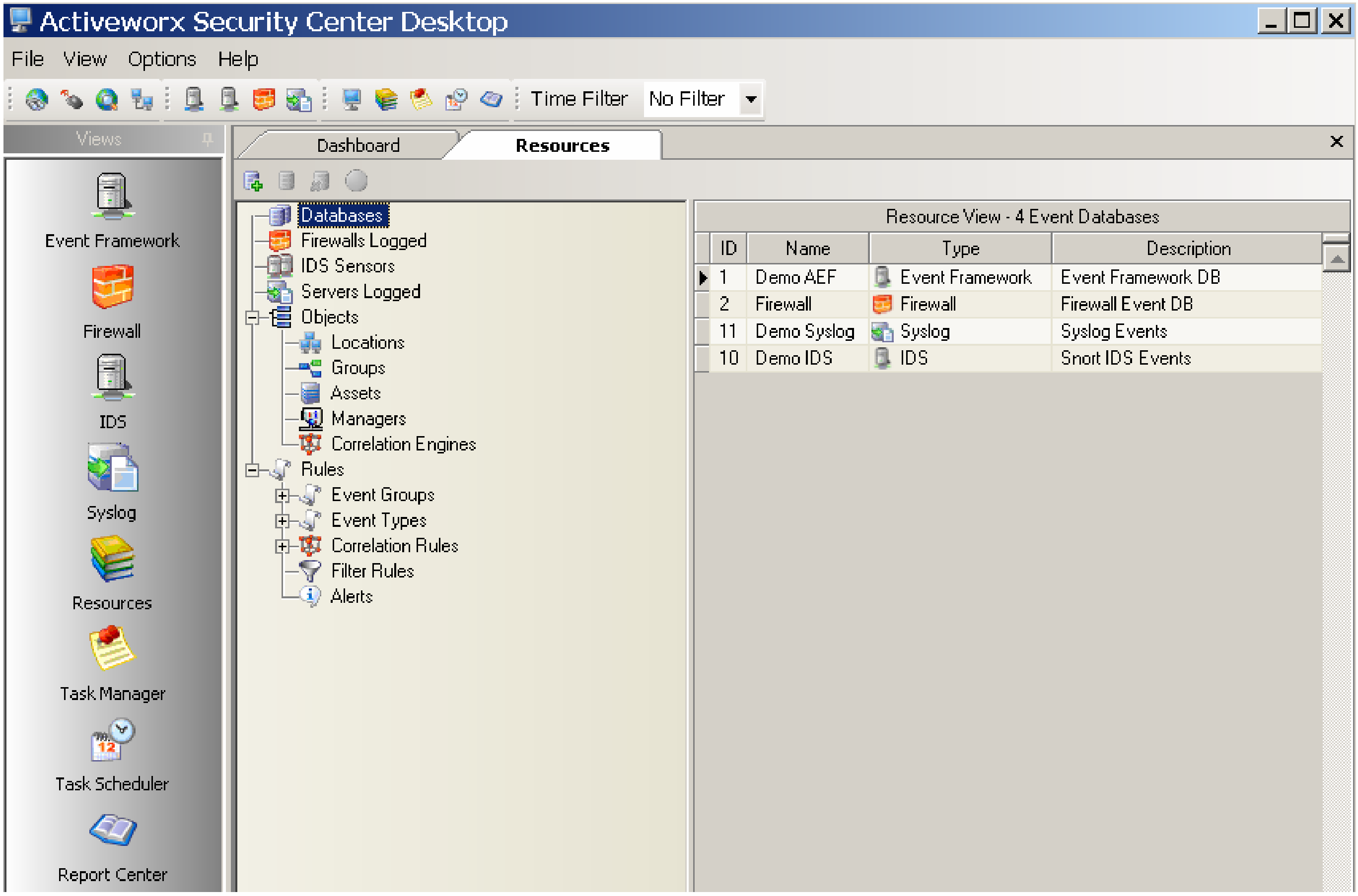


The ASC Desktop

Working with Resources and Databases

Upon completion of the Quick Install Guide, you will have logged into the ASC Desktop and notice that the ASC Configuration Wizard has created the databases required for an administrator to begin logging events. The next step is to log into the primary database with the ASC Desktop, usually created and named by the Config Wizard as aw_asc. The primary database will hold most of the Desktop's configuration settings. From here we want to view what Resources are defined after the initial configuration. If during the wizard you defined Windows, Checkpoint, and Linux for example, as the types of devices you want to monitor, you can look into the MySQL data directory or at Enterprise Manager for MSSQL and see an aw_aef as well as an aw_fw database. Both of these extra databases are used as actual 'Event Databases' which will store the security events gathered by the Collector Modules for viewing, graphing, reporting and correlating.

If you haven't already log into the ASC Desktop & click the Resources Icon on the left or top toolbar. By default it will open to the Databases section and give a listing of the defined databases in ASC. If there is a need to view other databases in the future; this is where you add a new database to the ASC view.



Time Filter: No Filter

Resource View - 4 Event Databases

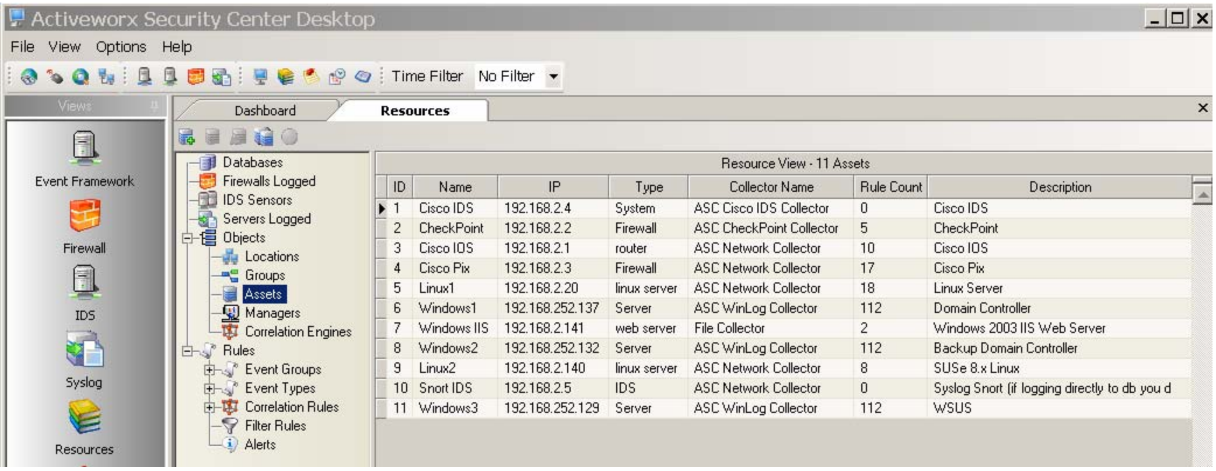
ID	Name	Type	Description
1	Demo AEF	Event Framework	Event Framework DB
2	Firewall	Firewall	Firewall Event DB
11	Demo Syslog	Syslog	Syslog Events
10	Demo IDS	IDS	Snort IDS Events

As you can see along the middle of the screenshot above there are quite a few things that are controlled and configured via the Resources module within the ASC Desktop. Whereas the other modules are usually for viewing, reporting, or creating tasks, Resources are where a large percentage of the actual ASC configuration takes place. Some of the features that can be configured via Resources include defining security devices (assets), configuring the ASC Manager, creating, modifying, and enabling Rules, defining groups for all types of Objects, as well as Correlation and Alerts.

Configuring Security Devices

During the Configuration Wizard you defined at least one or more security devices, or Assets, which you wanted to monitor for security events. From within Resources > Objects > Assets you will find those assets that were previously defined, and you have the opportunity to add, modify, or delete assets as necessary to monitor more or less devices on the network.

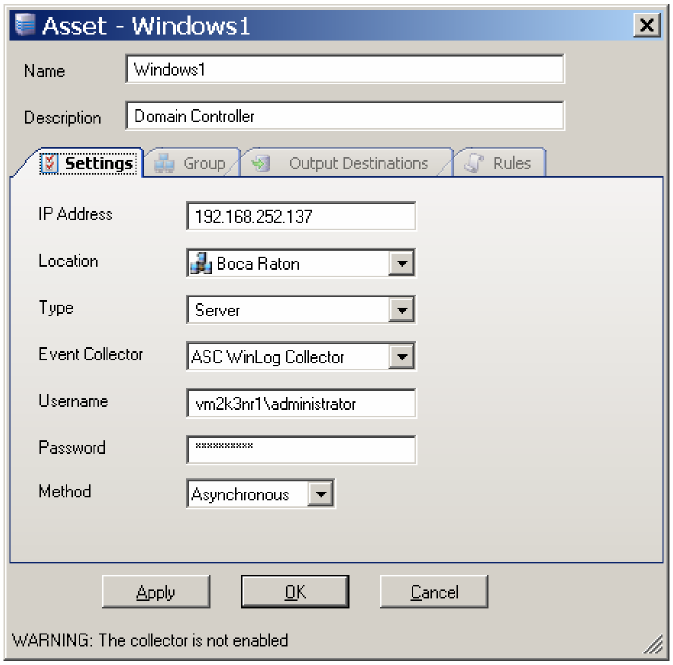
Below you’ll see a list of several devices that we have defined during our Configuration Wizard, as a quick example we will take a look at the settings for each of a Windows, Linux, and Firewall device type to illustrate the difference and similarities between them. The main items that must be defined within the assets **before** event collection are the *Collector type*, *Output destination*, and *Relevant rules*.



Resource View - 11 Assets

ID	Name	IP	Type	Collector Name	Rule Count	Description
1	Cisco IDS	192.168.2.4	System	ASC Cisco IDS Collector	0	Cisco IDS
2	CheckPoint	192.168.2.2	Firewall	ASC CheckPoint Collector	5	CheckPoint
3	Cisco IOS	192.168.2.1	router	ASC Network Collector	10	Cisco IOS
4	Cisco Pix	192.168.2.3	Firewall	ASC Network Collector	17	Cisco Pix
5	Linux1	192.168.2.20	linux server	ASC Network Collector	18	Linux Server
6	Windows1	192.168.252.137	Server	ASC WinLog Collector	112	Domain Controller
7	Windows IIS	192.168.2.141	web server	File Collector	2	Windows 2003 IIS Web Server
8	Windows2	192.168.252.132	Server	ASC WinLog Collector	112	Backup Domain Controller
9	Linux2	192.168.2.140	linux server	ASC Network Collector	8	SUSe 8.x Linux
10	Snort IDS	192.168.2.5	IDS	ASC Network Collector	0	Syslog Snort (if logging directly to db you d
11	Windows3	192.168.252.129	Server	ASC WinLog Collector	112	WSUS

Let’s begin with a Windows Server as shown below, double click your asset to view the Settings tab:



Name	Windows1
Description	Domain Controller
IP Address	192.168.252.137
Location	Boca Raton
Type	Server
Event Collector	ASC WinLog Collector
Username	vm2k3nr1\administrator
Password	**********
Method	Asynchronous

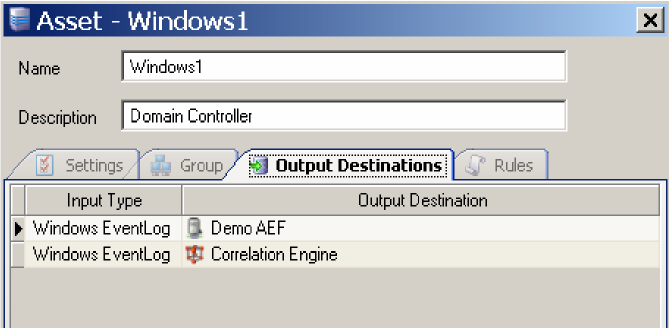
WARNING: The collector is not enabled

NOTE: Proper Windows user credentials are required in the Settings tab of the asset for the connection to and pulling of events from a Windows server on the network. Alternatively you can go to the properties of the ASC Manager Service in Windows and directly apply credentials into the Log-on As field, this is ideal if you will be using the same credentials to pull events for all of your Windows hosts.

This login requires WMI query rights to said host. You can use a tool called Wbemtest.exe from the Windows command line to test credentials for a Synchronous or Asynchronous WMI connection. Please see *Special Considerations for Windows Event Collection* on page 15.

All defined Assets within the Resources section of the ASC Desktop will have a few settings that need to be defined so that we can begin viewing events. Among these are:

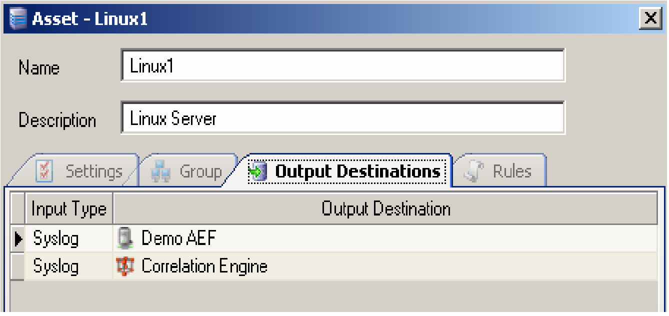
- **General Settings:** This is where you can define the type of Event Collector to be used to gather events from this specific asset, as well as enter Windows login credentials if necessary.
- **Group membership:** By grouping assets within the ASC Desktop you can make the application of rules, reporting and many other features much easier to implement.
- **Output Destination:** The output destination of an asset will determine what the collector will do with the events that it gathers from the network. An output destination is usually an event database of some kind running on MySQL or MSSQL, but can also be the Correlation Engine.
- **Rules:** The rules defined in this dialog will determine exactly which events the ASC Manager will collect and which it will just drop. One of the most powerful capabilities of ASC is rule creation, the ability to use regular expressions to filter through tons of data and find exactly which events of interest you would like to log, and which ones are just noise on the network.


Asset - Windows1

Name: Windows1

Description: Domain Controller

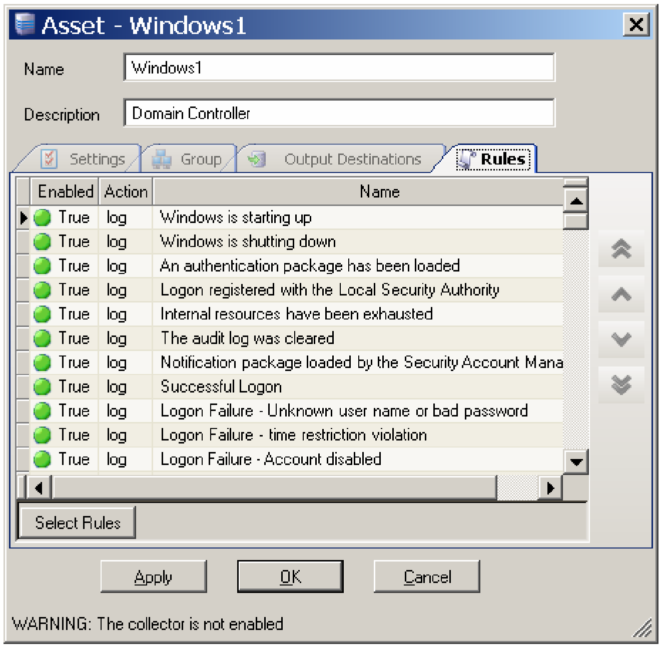
Input Type	Output Destination
Windows EventLog	Demo AEF
Windows EventLog	Correlation Engine


Asset - Linux1

Name: Linux1

Description: Linux Server

Input Type	Output Destination
Syslog	Demo AEF
Syslog	Correlation Engine

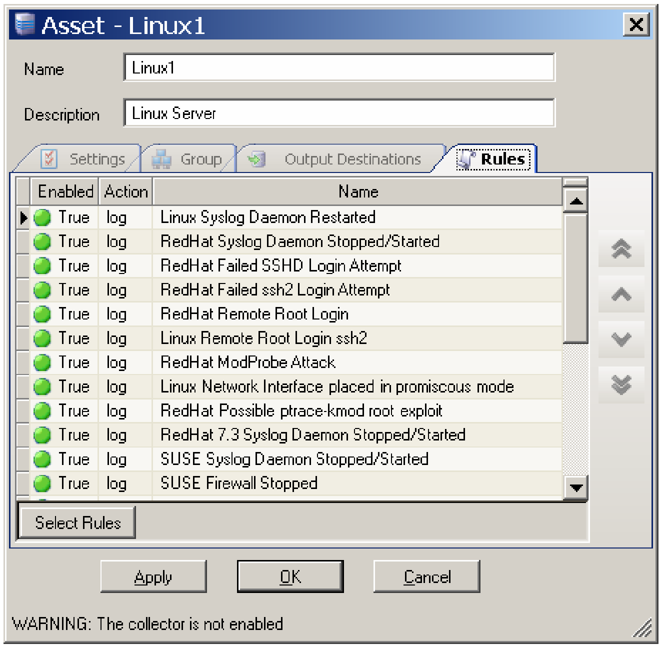

Asset - Windows1

Name: Windows1

Description: Domain Controller

Enabled	Action	Name
True	log	Windows is starting up
True	log	Windows is shutting down
True	log	An authentication package has been loaded
True	log	Logon registered with the Local Security Authority
True	log	Internal resources have been exhausted
True	log	The audit log was cleared
True	log	Notification package loaded by the Security Account Mana
True	log	Successful Logon
True	log	Logon Failure - Unknown user name or bad password
True	log	Logon Failure - time restriction violation
True	log	Logon Failure - Account disabled

WARNING: The collector is not enabled


Asset - Linux1

Name: Linux1

Description: Linux Server

Enabled	Action	Name
True	log	Linux Syslog Daemon Restarted
True	log	RedHat Syslog Daemon Stopped/Started
True	log	RedHat Failed SSHD Login Attempt
True	log	RedHat Failed ssh2 Login Attempt
True	log	RedHat Remote Root Login
True	log	Linux Remote Root Login ssh2
True	log	RedHat ModProbe Attack
True	log	Linux Network Interface placed in promiscous mode
True	log	RedHat Possible ptrace-kmod root exploit
True	log	RedHat 7.3 Syslog Daemon Stopped/Started
True	log	SUSE Syslog Daemon Stopped/Started
True	log	SUSE Firewall Stopped

WARNING: The collector is not enabled

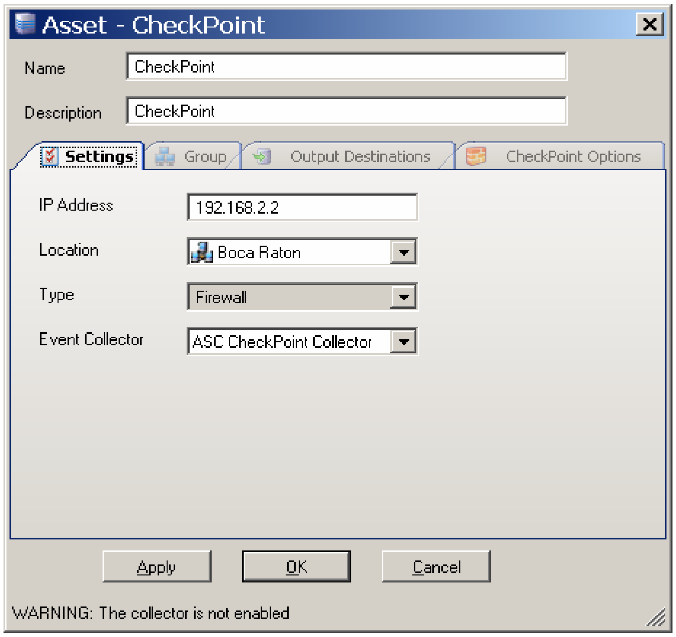
These diagrams display the typical set up for both a Windows and a Linux server as an Asset. The Linux server has different rules and can have different output destinations than the Windows server. Also on the Settings tab of your asset you'll notice that the Linux server uses the Network Collector, not the Winlog Collector. The Network Collector runs as a Windows service (one of the Collector Modules that an ASC Manager will be running) listening for Syslog messages and SNMP traps, typically on ports 514 and 162 UDP respectively. In this case the Linux and Windows server events are being put into both a database for logging and reporting (called the Activeworx Event Framework), as well as the Correlation Engine, for near real-time alerting and correlation.

With the ASC Desktop it's a simple matter to go to Resources > Databases and just right click and add a new database to put events in or add an existing database with Snort events which you'll be able to view without using a collector and without changing the schema of your IDS database (this is a Snort only feature).

Below is a screenshot of our Checkpoint Firewall, as you can see there is a vendor-specific collector specially for Checkpoint, this is because they have a proprietary logging protocol called OPSEC/LEA which the Checkpoint Collector needs to be able to parse so it can log to a database, in other words its different from standard Syslog or SNMP message, and the rules are different as well. However, you may notice that the Checkpoint firewall is also being inputted separately into a third location, its very own firewall database. This can be done for management, reporting, performance, or archival purposes – actually there are plenty of reasons why you may need to keep events in different databases.

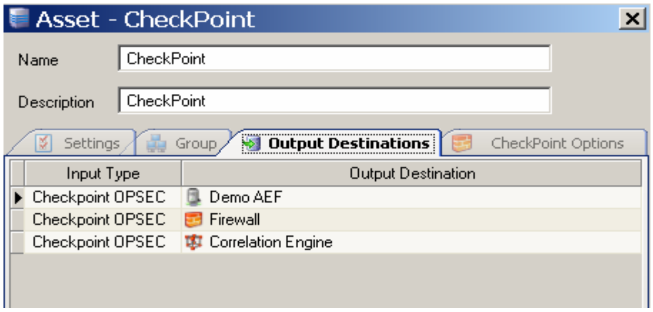
Common scenarios for when there may be a need to split the events coming for your assets into different event databases are:

- Placing firewall logs into its own ASC firewall database because it is designed to utilize the least amount of memory and provides much better performance than other database types.
- Placing IDS Events into the IDS database because IDS products like snort store the entire datagram and is obviously a very different event than a firewall permit or deny log.
- Placing events into a database that is close to the ASC Manager. The Scheduling Engine could then pickup events at scheduled intervals quickly and without utilizing much bandwidth.



Name: CheckPoint
Description: CheckPoint
IP Address: 192.168.2.2
Location: Boca Raton
Type: Firewall
Event Collector: ASC CheckPoint Collector

WARNING: The collector is not enabled



Name: CheckPoint
Description: CheckPoint

Input Type	Output Destination
Checkpoint OPSEC	Demo AEF
Checkpoint OPSEC	Firewall
Checkpoint OPSEC	Correlation Engine

Special Considerations for Windows Event Collection:

There are times that Windows may not allow WMI queries for one reason or another; in these cases you can take the following steps to help troubleshoot the issue:

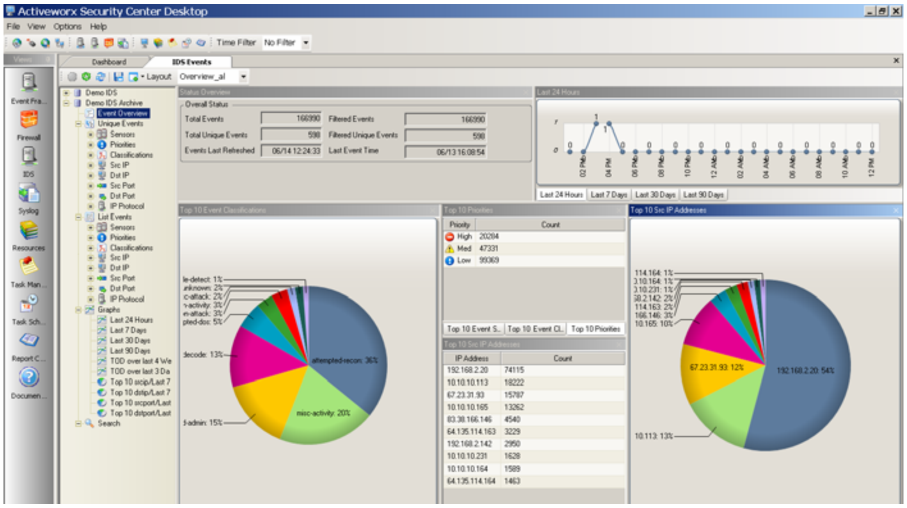
1. Open a Command Prompt and type in wbemtest.exe
2. Click Connect and replace the \root\default to \\10.1.1.31\root (sometimes its \default but in most cases its \\ip_address\root)
3. Type in your User credentials, same as in the ASC Desktop for your asset, and leave the Authority box blank but precede the username with a domain name i.e. demo\administrator.
4. Click Connect and your options should light up.
5. Select Asynchronous as your connection method and click on Enum Classes (**Some hosts may not work in Asynchronous mode. If this is the case, you can try Synchronous mode to see if this works. If it does you will want to configure this method for your asset**).
6. Click OK - if there is a response it works, if it fails WMI is not allowed from the local box to that server and you will either have to get a domain admin involved to check it out or use different user credentials.

NOTE: To ensure a proper test verify that the username in wbemtest is the same as within the asset or the Manager Service. If Wbemtest is successful but ASC is not retrieving Windows events, or you see a specific error within the ASC Manager log please contact technical support at 1-800-675-0729 or tech@crossteccorp.com.

Viewing and Analyzing Security Events

One of the most powerful screens within ASC is the Event Overview screen. The Event Overview screen is available for all databases that are being monitored whether it is IDS, Firewall, Syslog, or ASC Event Framework. You can now customize event panels to that the layout of your choosing to provide a bird's eye view of your security infrastructure. These include Top 10 lists for almost every category of event such as: Top 10 Protocols, Src/Dst IPs, Event Sensors, Rules, and much more. All of these text panels can also be shown as a graph, with all the same attributes. You also have the ability to select a small piece of the graph and view the event details of only that event or subset of events as well as easily and quickly email a group of events or correlate them with events that may have happened in another database right from the graph.

Next is a screenshot of our IDS Event Overview screen. You will notice along the left there are different categories which can switch to for more details on specific events or sensors or even run searches on our IDS database based on specific criteria.



Overall Status

Total Events	166990	Filtered Events	166990
Total Unique Events	598	Filtered Unique Events	598
Events Last Refreshed	06/14 12:24:33	Last Event Time	06/13 16:08:54

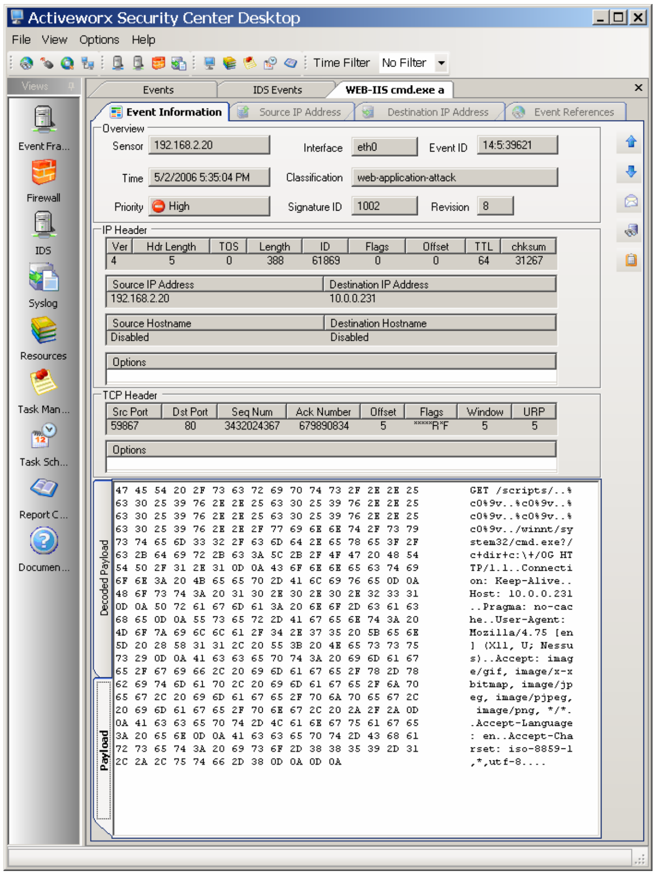
Priority	Count
High	20204
Med	47331
Low	99369

IP Address	Count
192.168.2.20	74115
10.10.10.113	18222
67.23.31.93	15787
10.10.10.165	13262
83.38.166.146	4540
64.135.114.163	3229
192.168.2.142	2950
10.10.10.231	1628
10.10.10.164	1589
64.135.114.164	1463

Assuming there is an interesting event that you would like to research a little further you can double click that event or group of events right from the Event Overview screen and do several things. Some of the most common actions taken to begin your analysis of a possible incident are:

- Use built-in IP tools such as NSlookup, WhoIS, Tracert, or Ping to find out more information.
- Use on-line references automatically looking up event details on vendor websites like Snort.org.
- Easily email events to groups within your organization or to like isc.sans.org for further analysis.
- Correlate events from one database which is storing events from one device with other databases storing events from other device types. For example you may see an IDS event that looks suspicious, so you may want to correlate that event based on Source IP with your firewall database to gather all the packets that match, and then correlate that event by Destination IP to view all the events that have recently come up on the actual Host that is the victim of the attack.

Another powerful way that ASC can help analyze events is by allowing the security administrator to drill down into the packet payload itself of an IDS event to automatically decode the hexadecimal and either display it to the screen, email it, copy it to the clipboard or correlate that event with events on other disparate security devices. Below is an example IDS event that triggered on a Web IIS attack, you can see the packet payload in hex on the left and the decoded packet on the right, you also get nice little breakdowns for each of the sections in the IP and TCP headers for quick and easy IDS event analysis.



Overview

Sensor 192.168.2.20 Interface eth0 Event ID 14:5:39621

Time 5/2/2006 5:35:04 PM Classification web-application-attack

Priority High Signature ID 1002 Revision 8

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	388	61869	0	0	64	31267

Source IP Address	Destination IP Address
192.168.2.20	10.0.0.231

Source Hostname	Destination Hostname
Disabled	Disabled

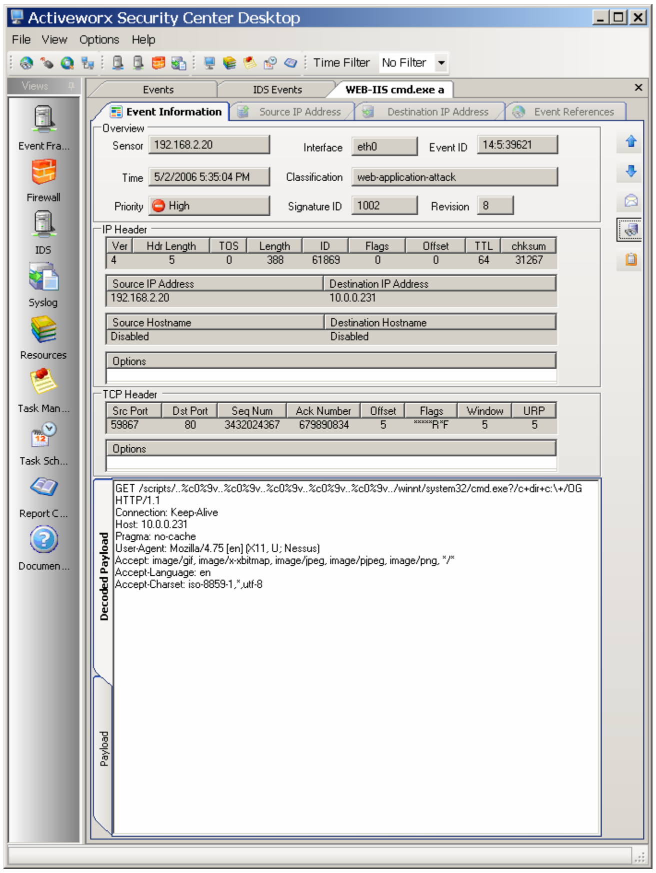
Options

TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
59867	80	3432024367	679890834	5	*****R*F	5	5

Options

```
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25       GET /scripts/..%
63 30 25 39 76 2E 2E 25 63 30 25 39 76 2E 2E 25       c0%9v..%c0%9v..%
63 30 25 39 76 2E 2E 25 63 30 25 39 76 2E 2E 25       c0%9v..%c0%9v..%
63 30 25 39 76 2E 2E 2F 77 69 6E 6E 74 2F 73 79       c0%9v../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F       stem32/cmd.exe?/
63 2B 64 69 72 2B 63 3A 5C 2B 2F 4F 47 20 48 54       c+dir+c:\+/OG HT
54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63 74 69       TP/1.1..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A       on: Keep-Alive..
48 6F 73 74 3A 20 31 30 2E 30 2E 30 2E 32 33 31       Host: 10.0.0.231
0D 0A 50 72 61 67 6D 61 3A 20 6E 6F 2D 63 61 63       ..Pragma: no-cac
68 65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20       he..User-Agent: 
4D 6F 7A 69 6C 6C 61 2F 34 2E 37 35 20 5B 65 6E       Mozilla/4.75 [en
5D 20 28 58 31 31 2C 20 55 3B 20 4E 65 73 73 75       ] (X11, U; Nessu
73 29 0D 0A 41 63 63 65 70 74 3A 20 69 6D 61 67       s)..Accept: imag
65 2F 67 69 66 2C 20 69 6D 61 67 65 2F 78 2D 78       e/gif, image/x-x
62 69 74 6D 61 70 2C 20 69 6D 61 67 65 2F 6A 70       bitmap, image/jp
65 67 2C 20 69 6D 61 67 65 2F 70 6A 70 65 67 2C       eg, image/pjpeg,
20 69 6D 61 67 65 2F 70 6E 67 2C 20 2A 2F 2A 0D        image/png, */*.
0A 41 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65       .Accept-Language
3A 20 65 6E 0D 0A 41 63 63 65 70 74 2D 43 68 61       : en..Accept-Cha
72 73 65 74 3A 20 69 73 6F 2D 38 38 35 39 2D 31       rset: iso-8859-1
2C 2A 2C 75 74 66 2D 38 0D 0A 0D 0A                   ,*,utf-8....
```



Overview

Sensor 192.168.2.20 Interface eth0 Event ID 14:5:39621

Time 5/2/2006 5:35:04 PM Classification web-application-attack

Priority High Signature ID 1002 Revision 8

IP Header

Ver	Hdr Length	TOS	Length	ID	Flags	Offset	TTL	chksum
4	5	0	388	61869	0	0	64	31267

Source IP Address	Destination IP Address
192.168.2.20	10.0.0.231

Source Hostname	Destination Hostname
Disabled	Disabled

Options

TCP Header

Src Port	Dst Port	Seq Num	Ack Number	Offset	Flags	Window	URP
59867	80	3432024367	679890834	5	*****R*F	5	5

Options

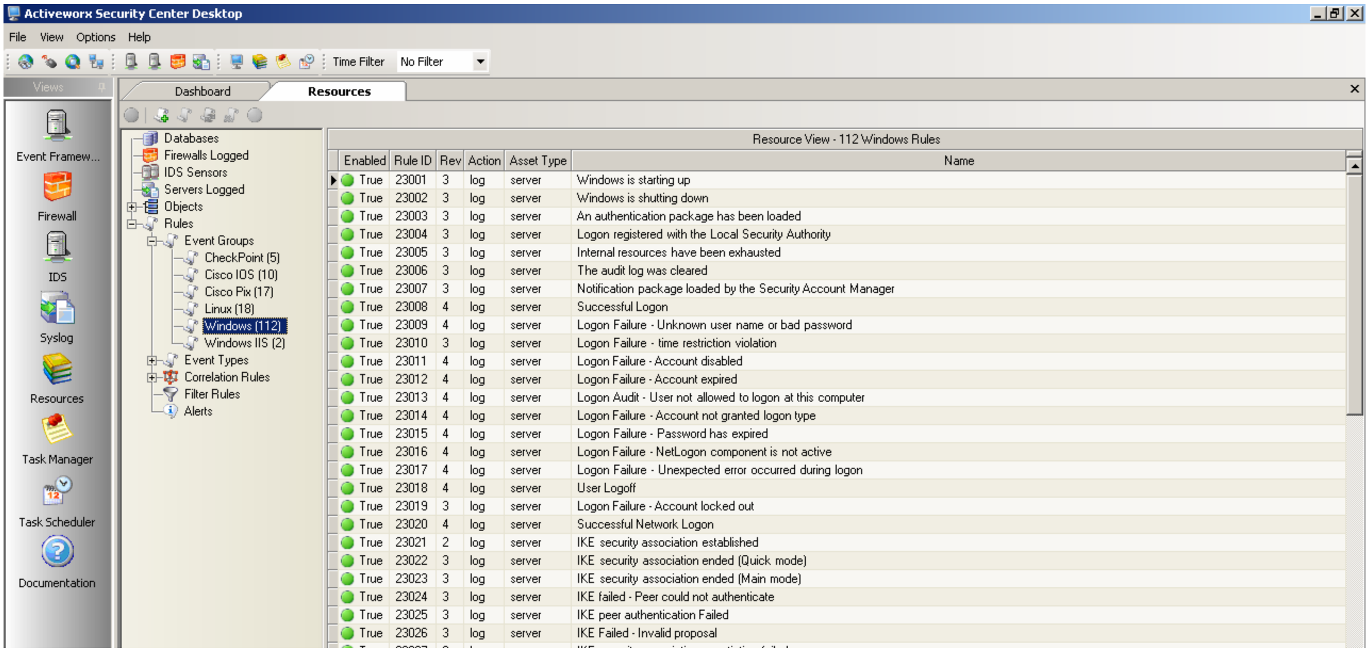
```
GET /scripts/..%c0%9v..%c0%9v..%c0%9v..%c0%9v..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\+/OG
HTTP/1.1
Connection: Keep-Alive
Host: 10.0.0.231
Pragma: no-cache
User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

Configuring Rules and Basic Alerting

Knowing when an event has occurred is imperative to security administrators; even more important is making sure that the event that has come in is indeed an important event or one that could be of interest to security administrators or auditors. The ASC Collectors provide rules-based alerting through standardized protocols such as email and Syslog. By default ASC will include some preconfigured rules for all device types that are supported, but usually there are specific events or applications that are unique to your environment, so in this case ASC allows the administrator to use a powerful regular expressions format to create new rules that will search for very specific events coming from a device or group of devices into the ASC Collectors. Each specific rule has the ability to be configured with an Alert. This alert can trigger in near real-time every time a rule is met and kick off an alert to an administrator or a manager that will increase incident response time and awareness.

Let's take Windows events as an example, but the following procedure can be used for adding rules to any device type. ASC can pick up any Windows Event Log entry from many servers across an enterprise and create an alert based on any event that triggers. It can also monitor events coming from many other assets such as firewalls, IDSes, and Syslog or SNMP enabled network devices all from a single console. Based on the format of the logs that are going to be retrieved, ASC uses a set of canned rules to determine if the event it sees is one of interest and should be logged to an ASC database, or if its just ignored and dropped. Once you have created an Asset within ASC, for example a Windows Application Server on your network, you may want to add or remove rules based on exactly what information you would like ASC to gather and make available to you. By default ASC 3.0 includes 112 rules that directly match all the Windows Security Events in Event Viewer. This means that with the default rule configuration for Windows Servers, ASC will only retrieve those events that go into the Security section of the Windows Event Log.

If an organization wants to monitor a different Windows Event Log such as the Application, System, Directory Services, or DNS event logs for a specific event or all of them, then a new rule must be created to match the information you would like ASC to retrieve. As an example we will add a rule that retrieves the entire Application Log from a Windows server. Go to Resources > Rules > Event Groups > Windows from with the ASC Desktop.

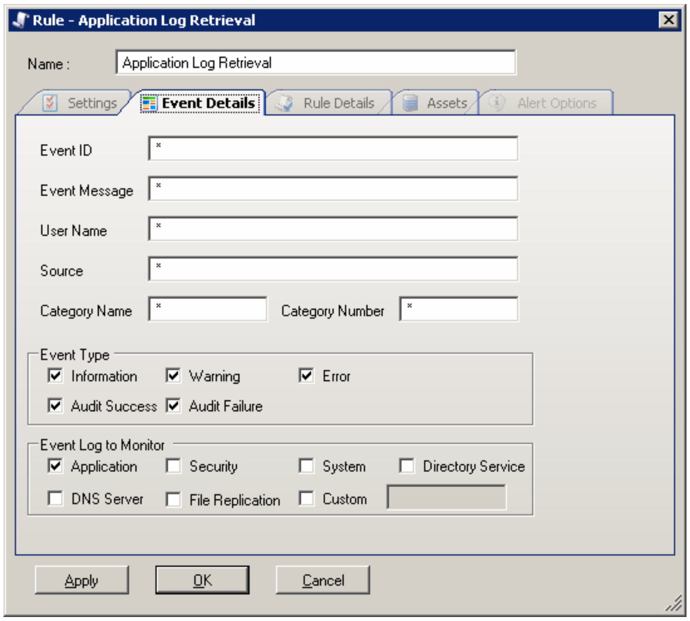


Resource View - 112 Windows Rules

Enabled	Rule ID	Rev	Action	Asset Type	Name
● True	23001	3	log	server	Windows is starting up
● True	23002	3	log	server	Windows is shutting down
● True	23003	3	log	server	An authentication package has been loaded
● True	23004	3	log	server	Logon registered with the Local Security Authority
● True	23005	3	log	server	Internal resources have been exhausted
● True	23006	3	log	server	The audit log was cleared
● True	23007	3	log	server	Notification package loaded by the Security Account Manager
● True	23008	4	log	server	Successful Logon
● True	23009	4	log	server	Logon Failure - Unknown user name or bad password
● True	23010	3	log	server	Logon Failure - time restriction violation
● True	23011	4	log	server	Logon Failure - Account disabled
● True	23012	4	log	server	Logon Failure - Account expired
● True	23013	4	log	server	Logon Audit - User not allowed to logon at this computer
● True	23014	4	log	server	Logon Failure - Account not granted logon type
● True	23015	4	log	server	Logon Failure - Password has expired
● True	23016	4	log	server	Logon Failure - NetLogon component is not active
● True	23017	4	log	server	Logon Failure - Unexpected error occurred during logon
● True	23018	4	log	server	User Logoff
● True	23019	3	log	server	Logon Failure - Account locked out
● True	23020	4	log	server	Successful Network Logon
● True	23021	2	log	server	IKE security association established
● True	23022	3	log	server	IKE security association ended (Quick mode)
● True	23023	3	log	server	IKE security association ended (Main mode)
● True	23024	3	log	server	IKE failed - Peer could not authenticate
● True	23025	3	log	server	IKE peer authentication Failed
● True	23026	3	log	server	IKE Failed - Invalid proposal

Step 1 - Add Rule: Open the ASC Desktop application and click on Resources > Rules > Windows > then right click and Add Rule.

Step 2 - **Configure Event Details:** After you configure the basic rule settings, switch to the Event Details tab and select the type of Windows Event Log you would like to monitor. If you leave an asterisk in every column ASC will retrieve the entire event log; however, should you have a specific network application that is logging to the Windows Application Log or are trying to retrieve only very specific events from one of the other logs, this rule can be easily configured based on parameters shown below.



Rule - Application Log Retrieval

Name : Application Log Retrieval

Event ID: *

Event Message: *

User Name: *

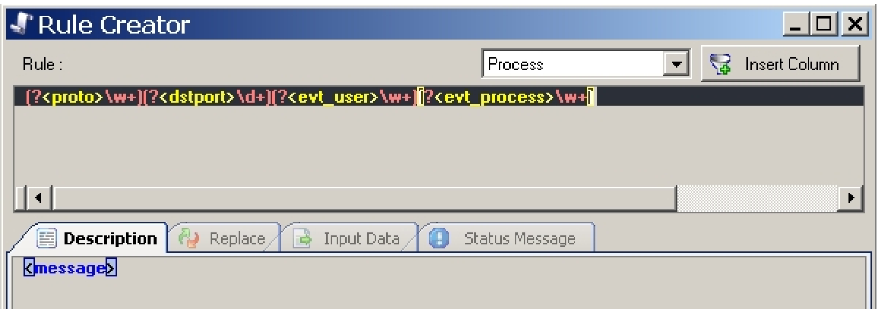
Source: *

Category Name: * Category Number: *

Event Type
☑ Information ☑ Warning ☑ Error
☑ Audit Success ☑ Audit Failure

Event Log to Monitor
☑ Application ☐ Security ☐ System ☐ Directory Service
☐ DNS Server ☐ File Replication ☐ Custom

Step 3 (Optional) **- Configure Rule Details:** If the options provided within the Event Details tab is not granular enough for your needs you can click on the Rule Details tab and use the built-in Rule Creator to create custom rules using regular expressions, the Rule Creator actually color coats the sections for ease of use.



Rule Creator

Rule : Process

```
(?<proto>\w+)(?<dstport>\d+)(?<evt_user>\w+)(?<evt_process>\w+)
```

<message>

Step 4 - Define Rule within the Assets: Next tab over called Assets gives you the ability to assign your new rule to any assets that have been defined within the Resources section of your ASC Desktop. This means we will be retrieving the Entire Windows Application Log from these servers we select here and only the Windows Security Log on the other servers for which we have not added the new rule.

Step 5 (Optional) - **Set up Alerts**. If you find a need to send an alert every time this rule fires then that can be easily configured from the Rule's Alert tab. Here you can setup email or Syslog events every time this rule is met by an event coming into your Windows Collector. If you have not yet created any alerts to choose from then you may have to save the rule first and configure some Alerts from the Resources > Alerts section of your ASC Desktop.

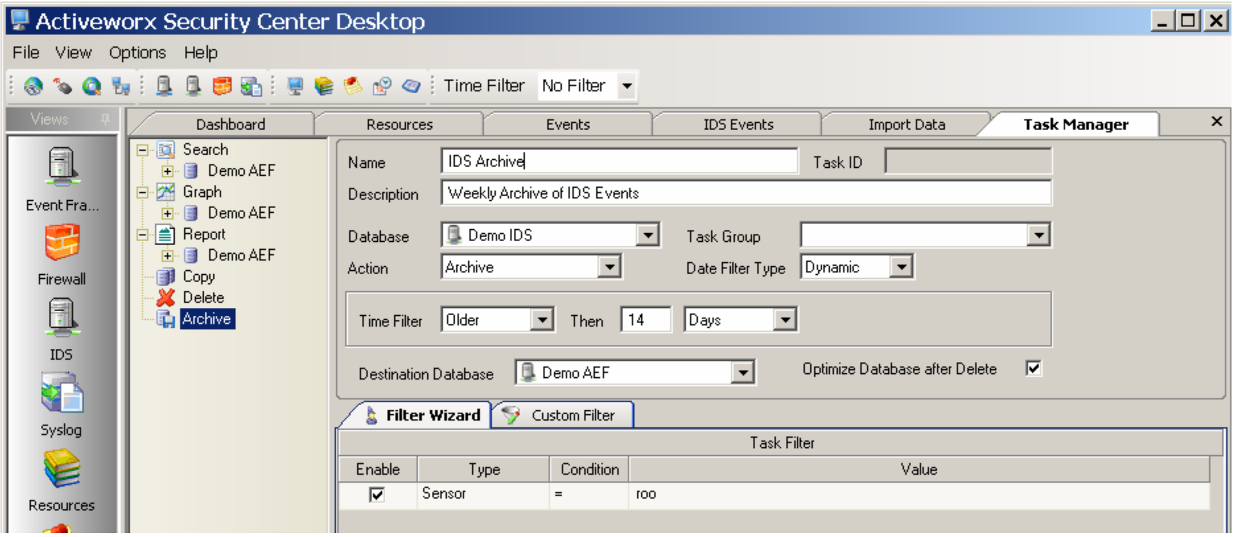
Finished! Once these steps have been taken the new Application Log Events on this particular group of servers should start coming up in the console view of the Event Framework database.

Archiving IDS Data

IDS data can become quite voluminous over time and usually the IDS analysis occurs in near real-time. However there may be scenarios where you will need to do some trend analysis over time or need to increase the performance of your IDS event database that the ASC Desktop and Manager uses. If you have several IDS sensors already logging to MySQL for example, then you may already have an archiving strategy for the events you don’t want to look at in your production database. If you have a need to create an archival strategy for your IDS data, meet compliance regulations, or review forensic information over a period of time; ASC can prove to be the tool that you need to make this happen easily and in an automated fashion. Some reasons for archiving IDS data could be:

- **Speed:** Make the event database faster, too many events obviously slows down database performance.
- **Regulatory Compliance:** Business requirements to keep events for 6 or 12 months but maybe you don't want them in your production db anymore
- **Trend Analysis:** If you don't really care about the events that are there but want to see what event trends looked like 6 months ago, then you can run reports on the archived data for a certain period in time.

To set up a task that will archive IDS data from one database to another is extremely easy to do by clicking on the **Task Manager**, right click **Archive** and click **Create New Task**. Simply choose your source and destination database as well as the time and event filters related to the events you would like to archive. As with any new task it can be scheduled to run with the use of a Scheduling Engine weekly or any specific time period.



Name: IDS Archive
Task ID:
Description: Weekly Archive of IDS Events
Database: Demo IDS
Task Group:
Action: Archive
Date Filter Type: Dynamic
Time Filter: Older Then 14 Days
Destination Database: Demo AEF
Optimize Database after Delete ☑

Task Filter

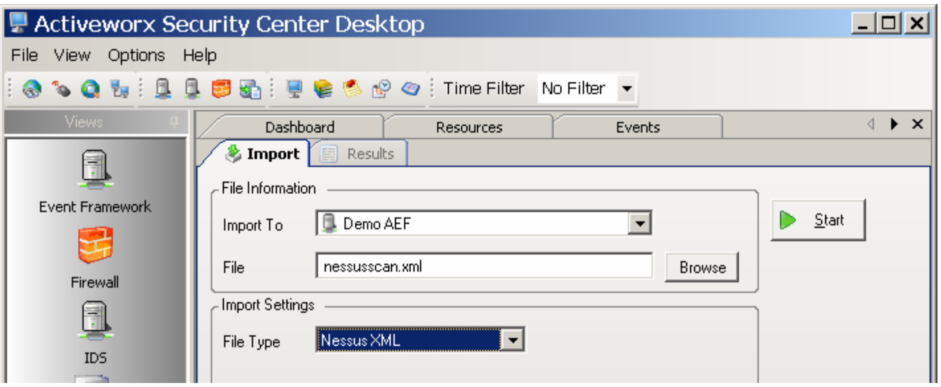
Enable	Type	Condition	Value
☑	Sensor	=	roo

Importing Vulnerability Scans with Nessus

Nessus.exe is an open source vulnerability scanner (the XML output) which is supported by ASC. So why run Nessus and import the data into an ASC Event Framework database? There are several compelling reasons to import vulnerability data such as:

- Correlating actual host vulnerabilities on your network with event data being collected by ASC.
- Viewing your security events and vulnerability information from a single, intuitive interface, instead of a command line or web interface.
- Running compliance reports and graphs on your vulnerability data just as easily as you do with IDS, Firewall, or Windows event data.

Combining your IDS data with vulnerability scans, a File Collector, and the Correlation Engine can automate the detection and correlation of near real-time events on your network. You can also alert on incidents that would otherwise go unnoticed. If you already run Nessus scans on a regular basis then all you have to do is click on Options > Import Data and browse to the XML scans you would like to import.



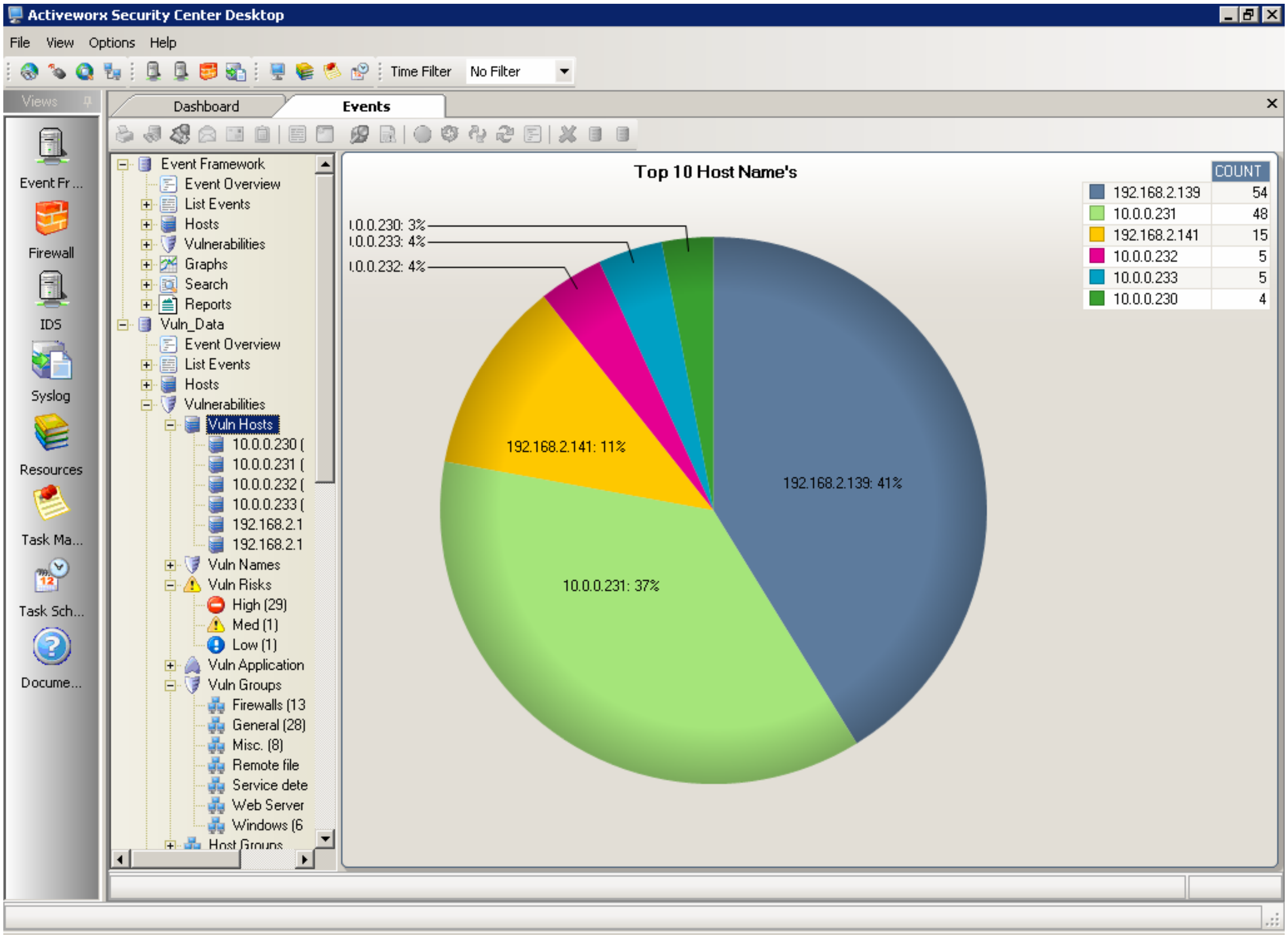
Time Filter: No Filter

Import To: Demo AEF

File: nessusscan.xml

File Type: Nessus XML

Below is a quick graphical view of the hosts that we are monitoring and have imported Nessus vulnerability scans for. Among the distinct categories that you can easily drill down into are individual hosts, vulnerability names, risks, applications and groups. Vulnerability reports are also a large piece of the puzzle when it comes to regulatory compliance and building network intelligence and awareness.



Top 10 Host Name's

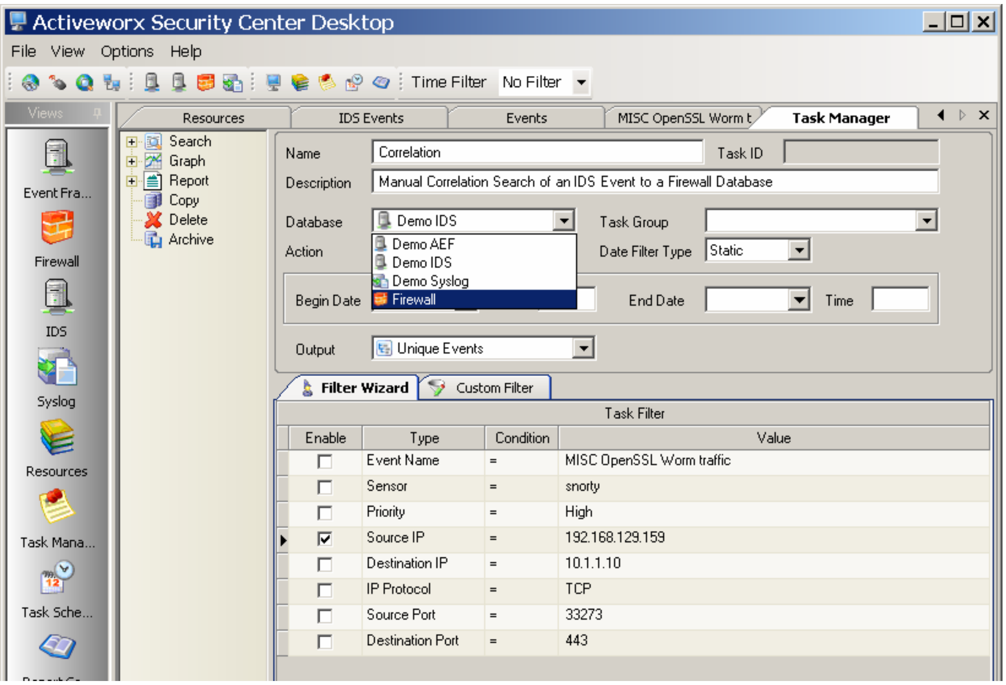
	COUNT
192.168.2.139	54
10.0.0.231	48
192.168.2.141	15
10.0.0.232	5
10.0.0.233	5
10.0.0.230	4

Event Correlation

Correlating Events across Security Devices

As discussed previously security event correlation is possibly the single most powerful feature within ASC. It allows a security administrator or auditor to get an event that arrives from IDS, correlate it with events that may have happened on any one of numerous firewalls and continues further to associate this threat information with events that have actually occurred on the end host system. So let’s take a look at manual event correlation from within ASC.

The first step in correlating events from within the ASC Desktop is to identify an event of interest. Say there is a high priority event triggered by your IDS, and you would like to see which firewall these events originated from. You can right click on an IDS right from the IDS Database > Event Overview and click Correlation Search. The Task Manager will appear with the fields of that event displayed in a Filter Wizard that will make it very easy to choose which field in the event you would like to correlate with the corresponding field in another event database. In this case we will select the Source IP field and switch the database to search on the top from IDS to Firewall. Then click Start.

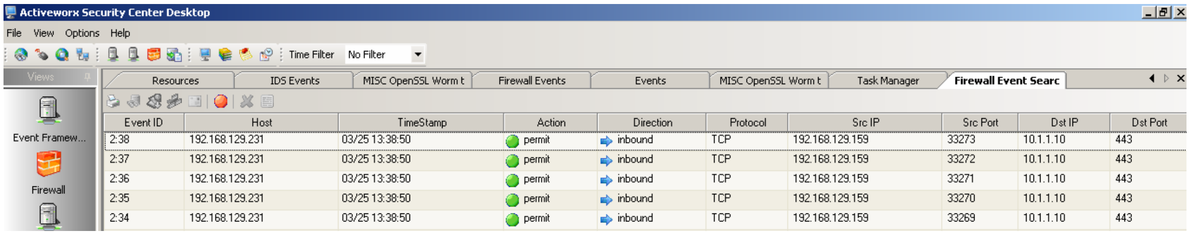


Name: Correlation
Task ID:
Description: Manual Correlation Search of an IDS Event to a Firewall Database
Database: Demo IDS
Task Group:
Action:
Date Filter Type: Static
Begin Date
End Date
Time
Output: Unique Events

Task Filter

Enable	Type	Condition	Value
□	Event Name	=	MISC OpenSSL Worm traffic
□	Sensor	=	snorty
□	Priority	=	High
☑	Source IP	=	192.168.129.159
□	Destination IP	=	10.1.1.10
□	IP Protocol	=	TCP
□	Source Port	=	33273
□	Destination Port	=	443

This will return all the matching permit/deny events from the Firewall that matches that Source. This will allow an administrator to build on the knowledge that an intrusion has occurred by knowing where it originated. But where did it go? Next we can select one or all of these events, right click and select Correlation Search. We will select Destination IP this time and our Event Framework database instead of the Firewall as that is where our host logs our and we are looking now for host events that match both our firewall logs as well as our newly triggered, high priority IDS event. The resulting search provides host logs and brings our intrusion analysis full circle across many disparate devices on the network.



Event ID	Host	TimeStamp	Action	Direction	Protocol	Src IP	Src Port	Dst IP	Dst Port
2:38	192.168.129.231	03/25 13:38:50	permit	inbound	TCP	192.168.129.159	33273	10.1.1.10	443
2:37	192.168.129.231	03/25 13:38:50	permit	inbound	TCP	192.168.129.159	33272	10.1.1.10	443
2:36	192.168.129.231	03/25 13:38:50	permit	inbound	TCP	192.168.129.159	33271	10.1.1.10	443
2:35	192.168.129.231	03/25 13:38:50	permit	inbound	TCP	192.168.129.159	33270	10.1.1.10	443
2:34	192.168.129.231	03/25 13:38:50	permit	inbound	TCP	192.168.129.159	33269	10.1.1.10	443

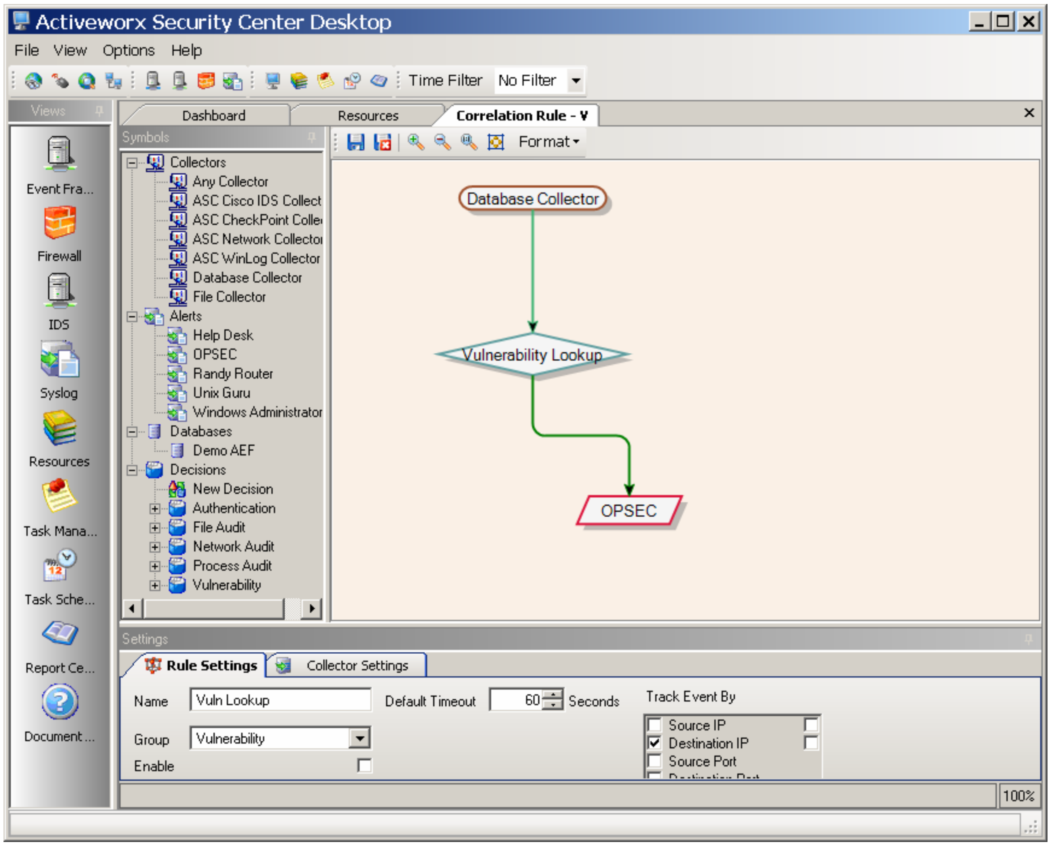
Automated Alerting with Correlation Rules

ASC's new Correlation Engine adds intelligent automation to the Activeworx Event Framework. It does this by allowing an administrator to use simple flow charts to create these complex correlation rules that we have just walked through manually in the previous section. With the Correlation Engine you have the ability to automatically correlate additional events coming in against existing data. When a suspect event is detected in one device's log file coming into our ASC collector, the software takes action based on those rules enabled within the asset to check other security information in the ASC system, making sure that the event is a real threat. It also has the ability to group events with commonalities, such as those involved in Brute Force attacks, into a single event with more in-depth information. To create a new correlation rule you would go to Resources > Rules > Correlation Rules within the ASC Desktop.

By double clicking one of these rules or just right clicking and selecting Add Rule we can see the basic dynamic of how a flow chart can be created using the concepts of correlation that we discussed earlier. Correlation rules can be very simple and serve the purpose of filtering through many events that are not of interest and only logging those that are, or they can become quite complex looking for very specific actions or combination of actions, within the events of many different devices and then generate alerts and logs accordingly.

A correlation rule can contain one or several of the following four component categories displayed on the left within the flow chart diagram we call a rule: Collectors, Alerts, Databases, and Decisions. We will look at these from a practical usage perspective.

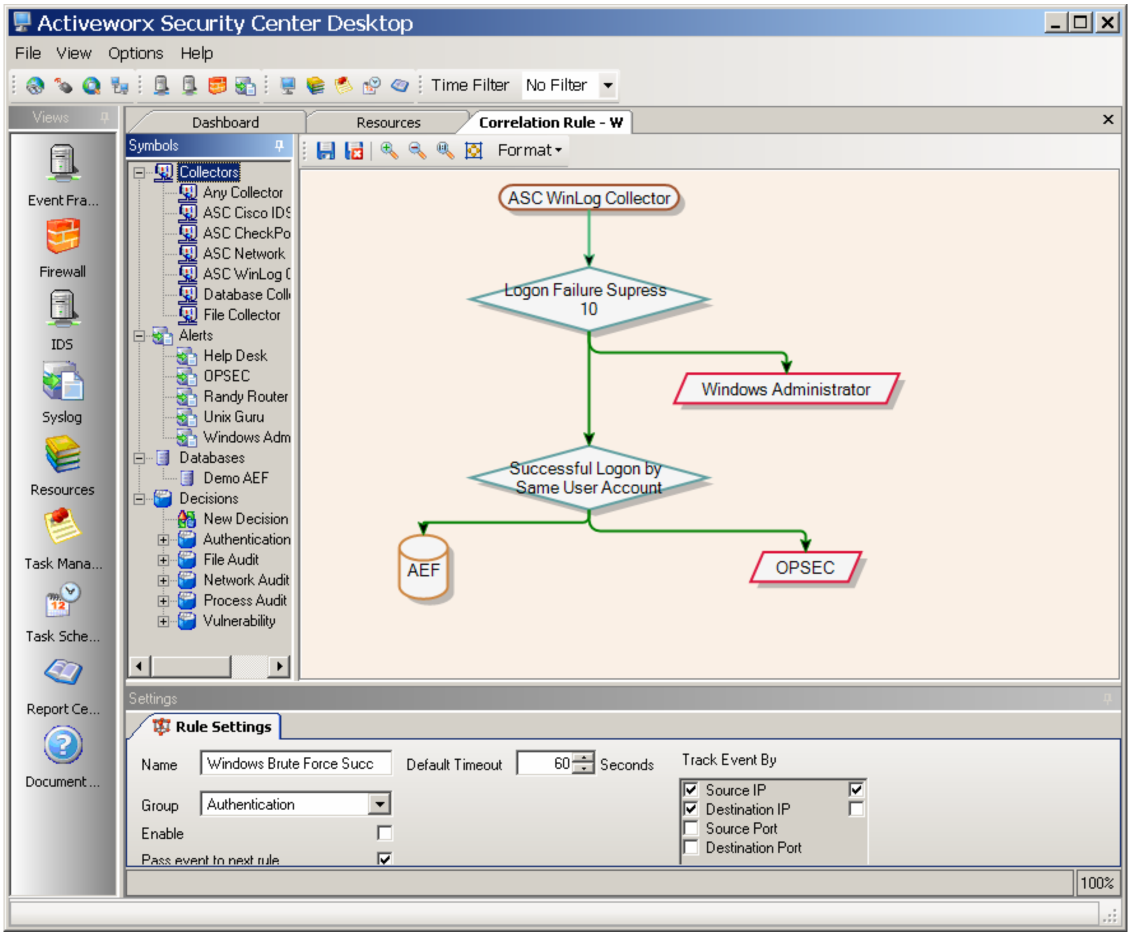
Here is a simple rule that pulls everything from an existing IDS database on the network using the Database Collector to run these IDS events through a vulnerability lookup based on Nessus Vulnerability Scans, these scans need to have been previously imported into the ASC Desktop as described in previous sections of this evaluator's guide.



Name: Vuln Lookup
Default Timeout: 60 Seconds
Group: Vulnerability
Enable ☐

Track Event By
☐ Source IP ☐
☑ Destination IP ☐
☐ Source Port

Next we get into describing a more complex rule which we have named Brute Force Successful – Windows. Because this one is more complex and uses at least one of each of the components types we will analyze this rule step by step and point out the points of interest and how we have managed to minimize the likelihood of false positives by using suppression features and multiple decisions.



Name: Windows Brute Force Succ
Default Timeout: 60 Seconds
Group: Authentication
Enable ☐
Pass event to next rule ☑

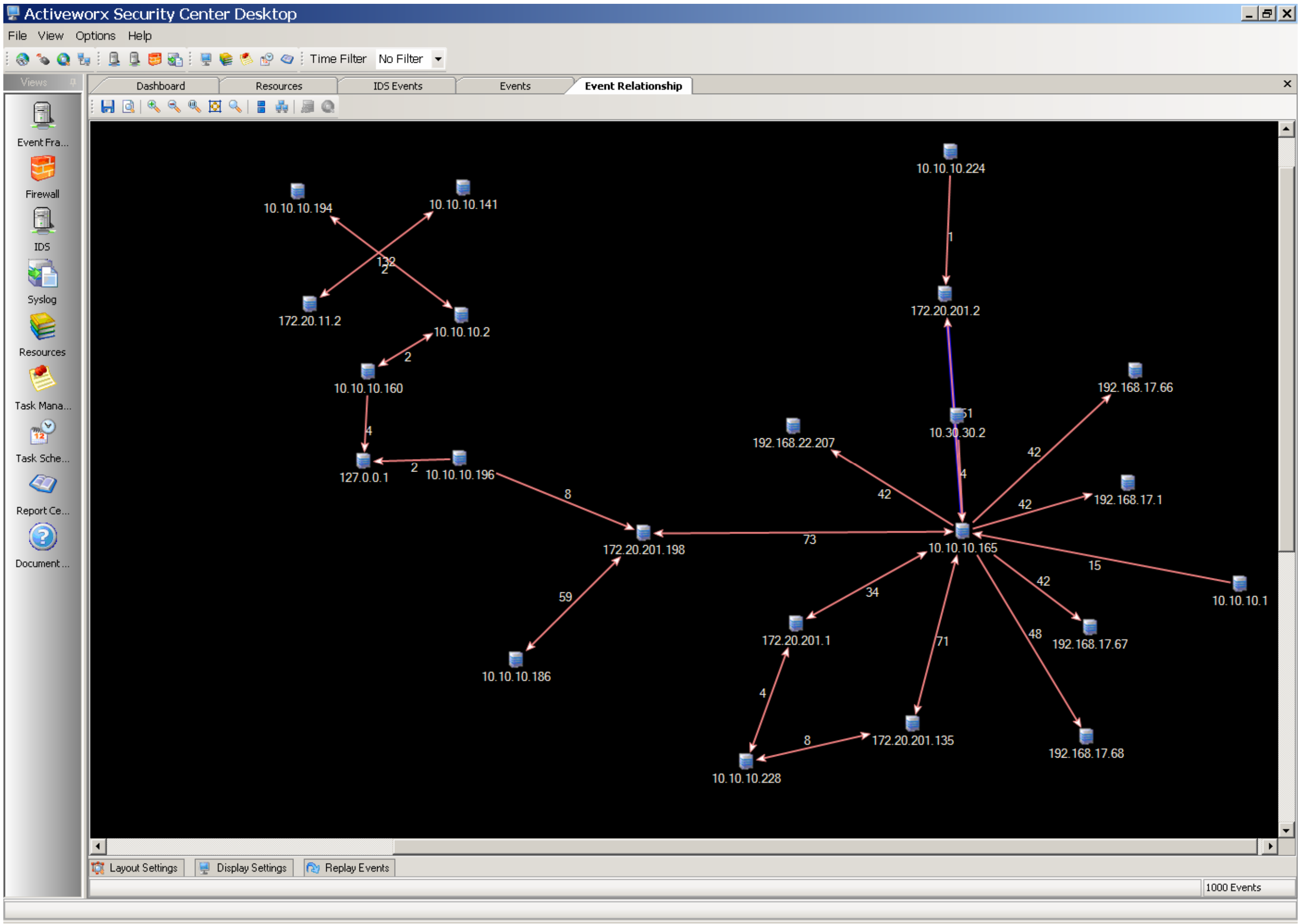
Track Event By
☑ Source IP ☑
☑ Destination IP ☐
☐ Source Port
☐ Destination Port

- **Collector:** All correlation rules will begin by defining what type of collector the Correlation Engine will monitor. It can be an individual collector or select Any Collector for the rule to monitor all collectors. In this case we are monitoring our Winlog Collector so all Windows events will be analyzed by this rule.
- **Decision 1:** Out first decision will analyze all events coming into the Winlog Collector and determine whether the event is a Logon Failure. We have set an option in the decision that will suppress ten failed logons from the same user name, source IP, and destination IP. So if there is a domain policy that says after five failed logons lock the account for two hours, this implies we should never see more than ten failed logons from the same user sequentially. If there is say 25 failed logons from the same user this can be an indication of a brute force logon attempt so we have set up an action to alert the Windows administrator by email.
- **Action 1 - Alert:** Send email to Windows admin with event details.
- **Decision 2:** Here we monitor the same user account after ten or more failed logons to see if that user ever succeeds. Its one thing to receive 25 failed logons and another to receive 25 failed logon followed by a successful one, indicating possible success of the brute force attack.
- **Action 2 - Log:** After the second decision has been met we decide that not only was that one email alert sent out but at this point we want to log the fact that this second decision was met to a database, this will help with keeping an audit trail of the attack.
- **Action 3 - Alert:** Not only have we decided to log the fact that this type of brute force attack was successful but we have set this rule up to fire a second alert email, this time to our incident response team for further investigation.

Event Visualization and Reporting

One of Activeworx Security Center's strengths comes in its ability to transform textual data and present it in a visual fashion, in the form of diagrams, graphs and reports.

Event Relationship Diagrams



Event Relationship Diagrams can be created by selecting (highlighting) multiple events from any list of events within ASC Desktop. After a selection is made, right-clicking on the highlighted area will present a menu where you can then left click on the "Diagram Events" option. ASC will then take those events and reconstruct the portion of your network that was involved in those events.

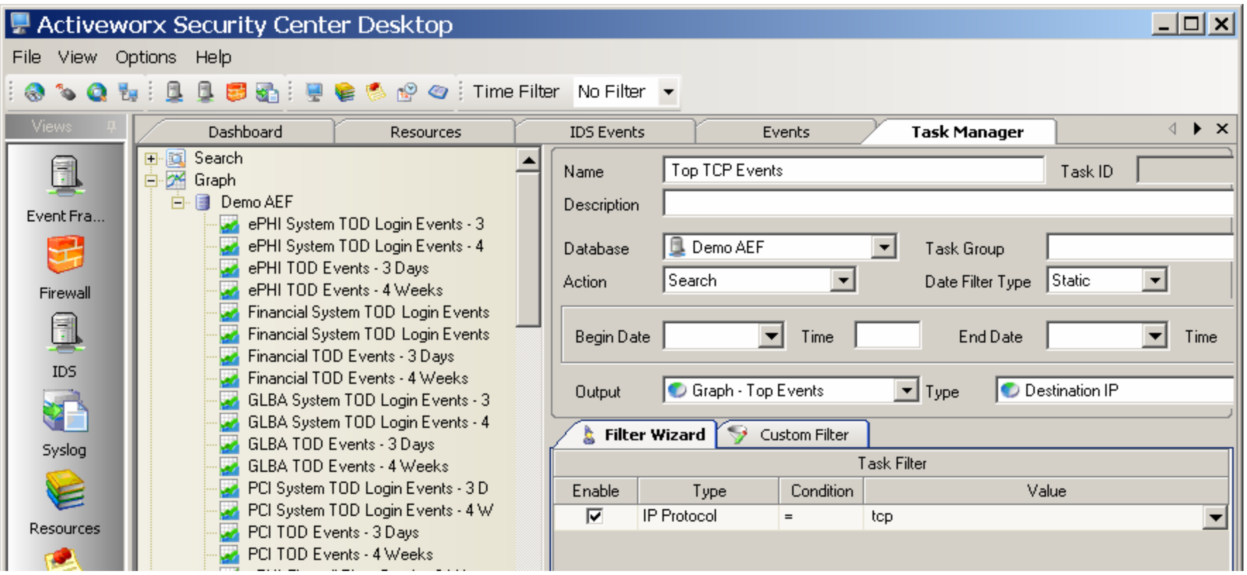
This will produce a diagram similar to the one above. The number next to the routes indicates the number of events that flowed between the two nodes and by right-clicking on the routes or the nodes you may view the events for that item.

You have the option of modifying how the diagram is drawn by using the "Layout Settings" tab and modifying background and route colors based on different criteria using the "Display Settings" tab.

The "Replay Events" tab is one of the most powerful features within ASC. The Replay Events feature will allow you to replay the events as they occurred in real-time. The route for each event will be highlighted as it occurs. You have the option of stepping through the events or auto-replay. Information about each event will be displayed as you progress between events.

Graphs

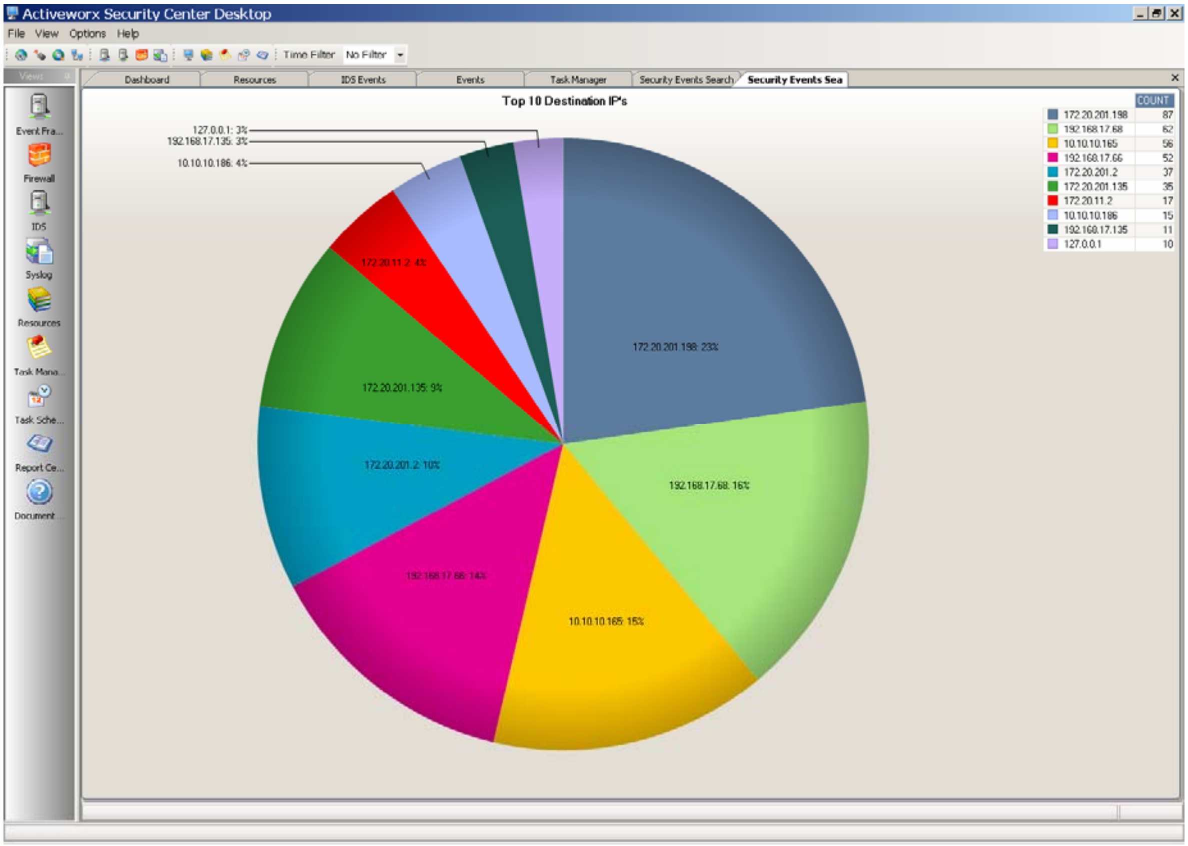
Another powerful feature of ASC is its ability to create an extensive array of graphs. ASC provides a wide variety of predefined graphs and gives you the ability to customize the graphs both in content and design. Through the Task Manager, you can select the type of graph by using Task Filters, the data that will be used to create the graph (as shown below). The appearance of the graph can then be modified by right-clicking anywhere in the graph area and bringing up the graph toolbar, where a full function graphing tool is provided. The graph can then be exported to disk for inclusion in reports or presentations. The graph is also interactive and by right-clicking on any of the segments, you may drill down into the underlying events.


Activeworx Security Center Desktop
File View Options Help
Time Filter No Filter
Views
Event Fra...
Firewall
IDS
Syslog
Resources
Dashboard
Resources
IDS Events
Events
Task Manager
Search
Graph
Demo AEF
ePHI System TOD Login Events - 3
ePHI System TOD Login Events - 4
ePHI TOD Events - 3 Days
ePHI TOD Events - 4 Weeks
Financial System TOD Login Events
Financial System TOD Login Events
Financial TOD Events - 3 Days
Financial TOD Events - 4 Weeks
GLBA System TOD Login Events - 3
GLBA System TOD Login Events - 4
GLBA TOD Events - 3 Days
GLBA TOD Events - 4 Weeks
PCI System TOD Login Events - 3 D
PCI System TOD Login Events - 4 W
PCI TOD Events - 3 Days
PCI TOD Events - 4 Weeks
Filter Wizard
Custom Filter

Name: Top TCP Events
Task ID:
Description:
Database: Demo AEF
Task Group:
Action: Search
Date Filter Type: Static
Begin Date: Time: End Date: Time:
Output: Graph - Top Events
Type: Destination IP

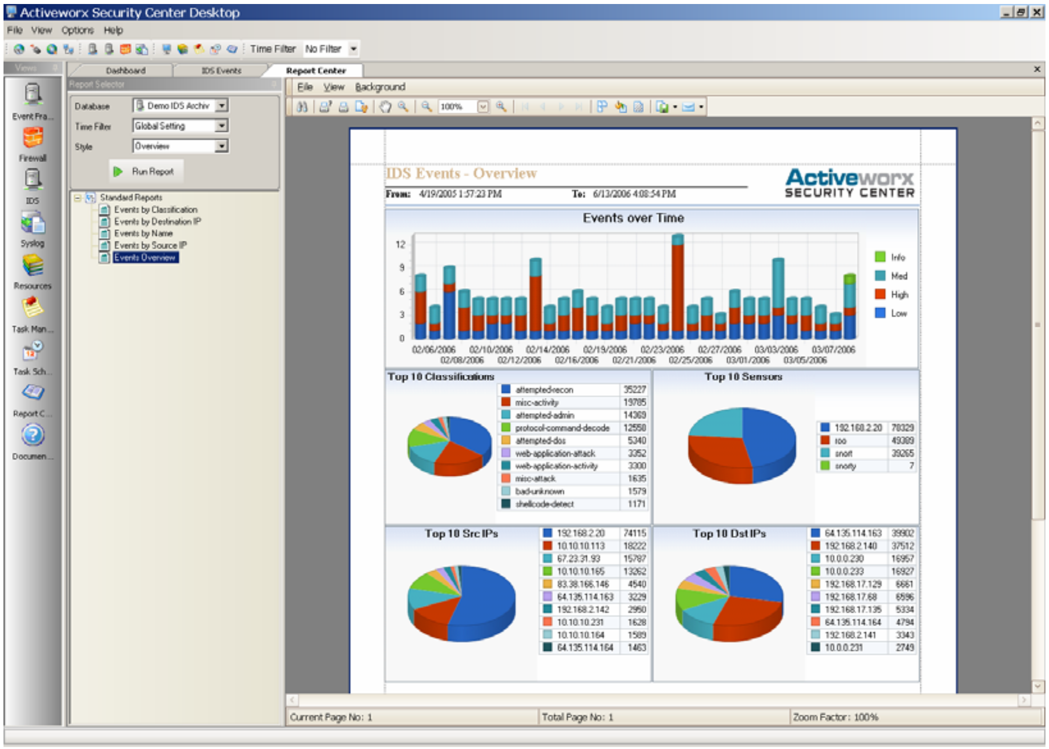
Task Filter

Enable	Type	Condition	Value
☑	IP Protocol	=	tcp



Reports

With so many compliance requirements, reporting becomes a critical feature for any SIM product. ASC comes with a large library of pre-defined reports and for those with specific compliance requirements (e.g. Sarbanes-Oxley, GLBA, HIPAA and PCI), several dozen pre-defined searches, graphs, diagrams and reports come standard with the package. By assigning the various servers and devices to reporting groups you can efficiently create reports that include all of the devices involved in a specific compliance requirement. As with graphs, the Task Manager can be used to select the type of report to be run and, by using Task Filters, the data that will be included or excluded from the report. For more complex selection criteria ASC also has a Custom Filters option where customers can create their own filters by using standard SQL language. Customized reports can be saved and reused at any time. Reports can be graphical in nature or in text (as seen above) depending on the type of report.



Database: Demo IDS Archiv

Time Filter: Global Setting

Style: Overview

IDS Events - Overview

From: 4/19/2005 1:57:23 PM To: 6/13/2006 4:08:54 PM

Top 10 Classifications

attempted-recon	35227
misc-activity	19785
attempted-admin	14369
protocol-command-decode	12558
attempted-dos	5340
web-application-attack	3352
web-application-activity	3300
misc-attack	1635
bad-unknown	1579
shellcode-detect	1171

Top 10 Sensors

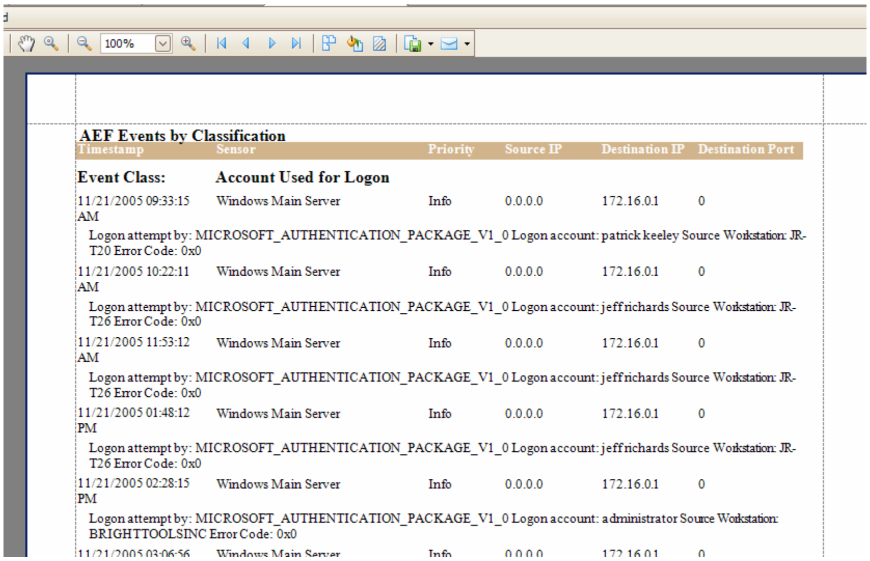
192.168.2.20	78329
roo	49389
snort	39265
snorty	7

Top 10 Src IPs

192.168.2.20	74115
10.10.10.113	18222
67.23.31.93	15787
10.10.10.165	13262
83.38.166.146	4540
64.135.114.163	3229
192.168.2.142	2950
10.10.10.231	1628
10.10.10.164	1589
64.135.114.164	1463

Top 10 Dst IPs

64.135.114.163	39902
192.168.2.140	37512
10.0.0.230	16957
10.0.0.233	16927
192.168.17.129	6661
192.168.17.68	6596
192.168.17.135	5334
64.135.114.164	4794
192.168.2.141	3343
10.0.0.231	2749

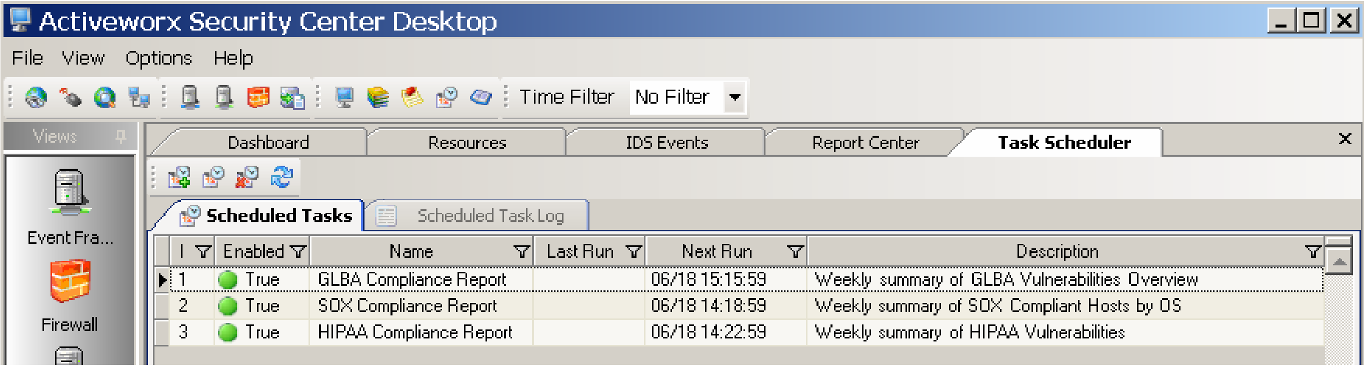


AEF Events by Classification

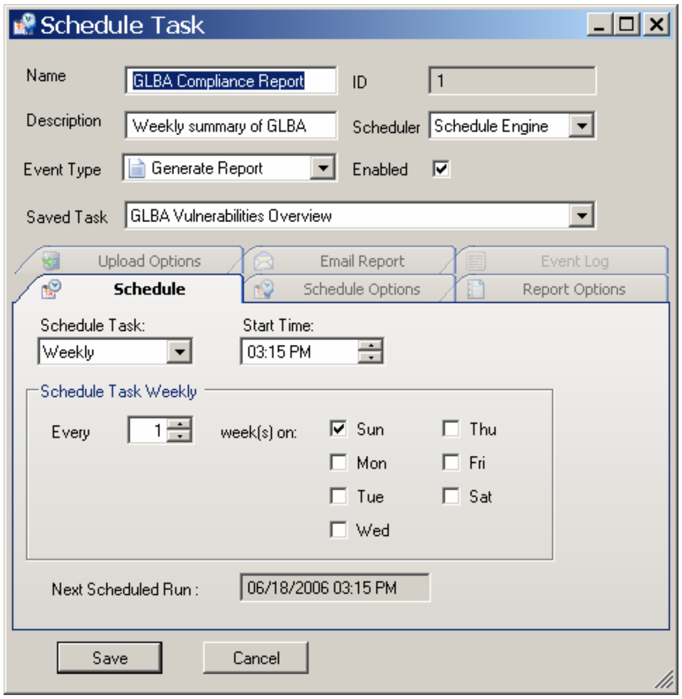
Timestamp	Sensor	Priority	Source IP	Destination IP	Destination Port
Event Class:	**Account Used for Logon**				
11/21/2005 09:33:15 AM	Windows Main Server	Info	0.0.0.0	172.16.0.1	0
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: patrick keeley Source Workstation: JR-T20 Error Code: 0x0					
11/21/2005 10:22:11 AM	Windows Main Server	Info	0.0.0.0	172.16.0.1	0
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: jeffrichards Source Workstation: JR-T26 Error Code: 0x0					
11/21/2005 11:53:12 AM	Windows Main Server	Info	0.0.0.0	172.16.0.1	0
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: jeffrichards Source Workstation: JR-T26 Error Code: 0x0					
11/21/2005 01:48:12 PM	Windows Main Server	Info	0.0.0.0	172.16.0.1	0
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: jeffrichards Source Workstation: JR-T26 Error Code: 0x0					
11/21/2005 02:28:15 PM	Windows Main Server	Info	0.0.0.0	172.16.0.1	0
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon account: administrator Source Workstation: BRIGHTTOOLSINC Error Code: 0x0					
11/21/2005 03:06:56	Windows Main Server	Info	0.0.0.0	172.16.0.1	0

Scheduling Reports

While having a comprehensive set of reports is important, running them on a manual basis would be time consuming and would lead to reports not being run or not being distributed properly, requiring a large amount of time to accomplish and producing inconsistencies. To facilitate the running of reports (and other tasks) and distributing them, ASC provides a Scheduling Engine that will automatically run tasks based on customer requirements. Customers can have the reports scheduled to run overnight and by morning have them distributed to the right people, all automatically. Any saved task can be scheduled to run and, in the case of reports, ASC gives several options for output format (e.g. HTML for use on web pages, PDF, MS Word, Excel, RTF etc.) and options for distributing the report (e.g. Upload to a server with standard or secure-copy, E-mail report or E-mail a notice that the report is complete, typically used when uploading report to a server). Tasks may be scheduled hourly, daily, weekly, monthly or just once. A log is also kept of previously run tasks to insure correct completion and identification of errors. Below is an illustration of some scheduled tasks with an overview of the available scheduling options and output formats.



I	Enabled	Name	Last Run	Next Run	Description
1	True	GLBA Compliance Report		06/18 15:15:59	Weekly summary of GLBA Vulnerabilities Overview
2	True	SOX Compliance Report		06/18 14:18:59	Weekly summary of SOX Compliant Hosts by OS
3	True	HIPAA Compliance Report		06/18 14:22:59	Weekly summary of HIPAA Vulnerabilities

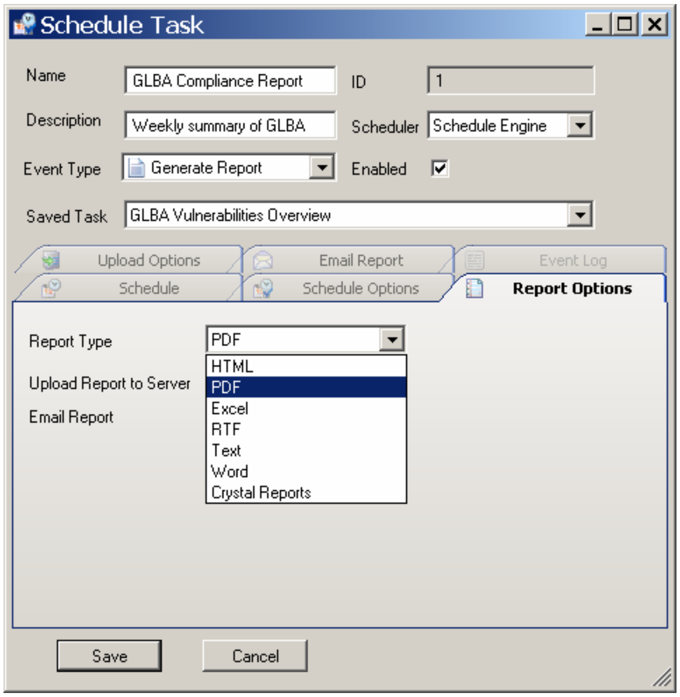


Name: GLBA Compliance Report ID: 1
Description: Weekly summary of GLBA Scheduler: Schedule Engine
Event Type: Generate Report Enabled: ☑
Saved Task: GLBA Vulnerabilities Overview

Schedule Task: Weekly Start Time: 03:15 PM

Every 1 week(s) on: ☑ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Next Scheduled Run : 06/18/2006 03:15 PM



Name: GLBA Compliance Report ID: 1
Description: Weekly summary of GLBA Scheduler: Schedule Engine
Event Type: Generate Report Enabled: ☑
Saved Task: GLBA Vulnerabilities Overview

Report Type: PDF
Upload Report to Server
Email Report

Conclusion

Activeworx Security Center (ASC) is a high-quality, low-cost, security information management (SIM) software solution that collects, normalizes and analyzes data from virtually any security device from any vendor. At the heart of Activeworx is the powerful Activeworx Event Framework (AEF) database which recognizes event data from your various vendor devices such as Firewalls, IDS, IPS, Syslog, SNMP, Vulnerability Assessment, Antivirus, Routers, Switches, VPN's, Windows Event Logs, and more. ASC supplies you with detailed security alerts, vital reports for investigations and regulatory compliance and deep forensics tools. ASC's intuitive design is both easy to install and easy to use offering you mission-critical security tools at an affordable price. After completing both the Quick Install Guide as well as this Evaluator's Guide you should have been able to thoroughly understand some of the features that are available to you as a security administrator, manager, and/or auditor. Among the primary features that we have highlighted in this guide for you are event correlation, compliance reporting, regular expression rule creation, IDS and vulnerability scan correlation, graphing and analyzing events, visualizing attack data, and alerting based on events of interest, as well as the automation of all of these security, management, and auditing tasks.

Additional set up will be necessary for a live production environment; however, the steps outlined here should get you through most of the evaluation process for ASC, as well as provide you with some tools to truly test the power of security information management. For additional help, you may visit our website at www.CrossTecCorp.com for FAQ page or view the on-line manual and tutorials found in the Help menu of the ASC Desktop.

You may also contact the Technical Support Group at (877) 512-4134 or by email tech@CrossTecCorp.com. Technical support is provided free of charge during the evaluation period and is included in the maintenance support if you're an existing customer. In other words, it's free.

We at CrossTec, Inc. and Activeworx, Inc. would like to take this opportunity to thank you for evaluating our software.