SNARE

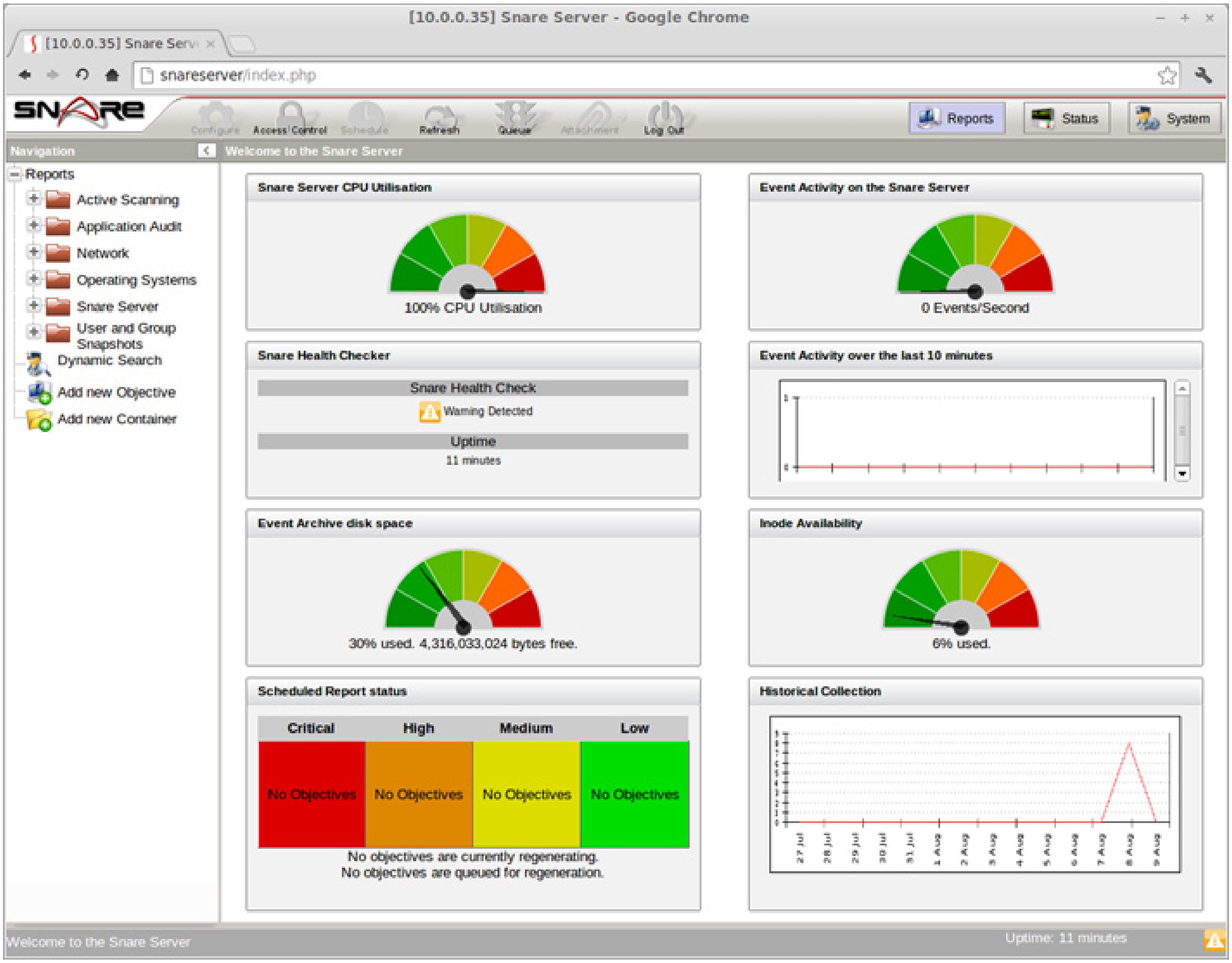
System iNtrusion Analysis & Reporting Environment

SNARE Server Version 6

Snare from InterSect Alliance, is an Enterprise level Security Event Mangement system. It is comprised of two toolsets, a robust central audit event collection, analysis, reporting and archiving tool (the Snare Sever) and the Enterprise Snare Agents which ensures collection of event logs from a number of operating systems, applications, as well as custom event logs.

With the release of Version 6.0 of the Snare Server a range of new functionality and features provides an excellent platform for users to meet key organizational security objectives

New User Interface:



Welcome to the Snare Server

Snare Server CPU Utilisation

100% CPU Utilisation

Event Activity on the Snare Server

0 Events/Second

Snare Health Checker

Snare Health Check

Warning Detected

Uptime

11 minutes

Event Activity over the last 10 minutes

Event Archive disk space

30% used. 4,316,033,024 bytes free.

Inode Availability

6% used.

Scheduled Report status

Critical	High	Medium	Low
No Objectives	No Objectives	No Objectives	No Objectives

No objectives are currently regenerating.
No objectives are queued for regeneration.

Historical Collection

Welcome to the Snare Server

Uptime: 11 minutes

For more information, contact your SNARE Server Sales Representative
snaresales@symtrex.com | 1-866-431-8972

Who's Watching Your Network?

The Snare Server user interface has been significantly redesigned for version 6, with a focus on simplifying navigation, and taking advantage of the features of modern browsers.

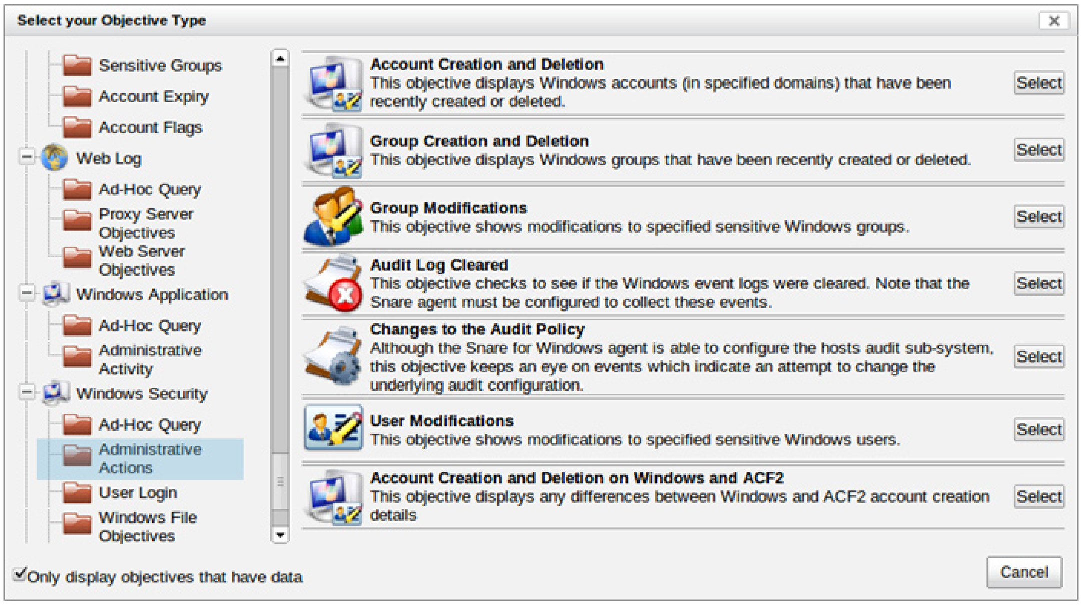
Drag & drop, pop-up windows, tabbed pages, and interactive updates all contribute to a modern streamlined environment that allows you to get on with the job of detecting security problems in your network, without the software getting in the way

Comprehensive Range of Reports

Enterprise Snare agents can collect from a massive variety of operating systems, services, and applications, as well as the server can receive from network devices, such as routers, switches, and firewall; and the reports available on the Snare Server reflect the complex ecosystem from which the log data is derived.

The Snare Server includes over 100 different reports spread amongst a wide range of categories, including administrative activity, sensitive file monitoring, user login activity, web proxy access, firewall and router monitoring, user and group checks, and many more.

The Snare Server now includes a unique feature of importing objectives or queries that have been built by your Snare Server support team, as well, as allows you to ensure that reports are standardized in a environment where multiple Snare Servers exist. Your Snare Server team can also generate new reports in response to new log sources, new security threats, and new regulatory requirements



Select your Objective Type

- Sensitive Groups
- Account Expiry
- Account Flags
- Web Log
  - Ad-Hoc Query
  - Proxy Server Objectives
  - Web Server Objectives
- Windows Application
  - Ad-Hoc Query
  - Administrative Activity
- Windows Security
  - Ad-Hoc Query
  - Administrative Actions
  - User Login
  - Windows File Objectives

Account Creation and Deletion
This objective displays Windows accounts (in specified domains) that have been recently created or deleted. Select

Group Creation and Deletion
This objective displays Windows groups that have been recently created or deleted. Select

Group Modifications
This objective shows modifications to specified sensitive Windows groups. Select

Audit Log Cleared
This objective checks to see if the Windows event logs were cleared. Note that the Snare agent must be configured to collect these events. Select

Changes to the Audit Policy
Although the Snare for Windows agent is able to configure the hosts audit sub-system, this objective keeps an eye on events which indicate an attempt to change the underlying audit configuration. Select

User Modifications
This objective shows modifications to specified sensitive Windows users. Select

Account Creation and Deletion on Windows and ACF2
This objective displays any differences between Windows and ACF2 account creation details Select

☑ Only display objectives that have data

Cancel

Users of previous versions of the Snare Server will find the range of reports very familiar, but will also discover that the updated query and output flexibility greatly expands the utility of reports.

Powerful Query and Output Option

The Snare Server's objective configuration interface starts off simple, and grows in capability and flexibility as you add filters, and output components to the mix.

Matching logs of interest is made easier with a query definition system that utilizes modern browser capabilities to provide a simple user interface, which still allows you to define complex queries.

The ability to use modular output components means that you can choose to have your output as sparse, or as complex as you need in order to meet your key reporting requirements.

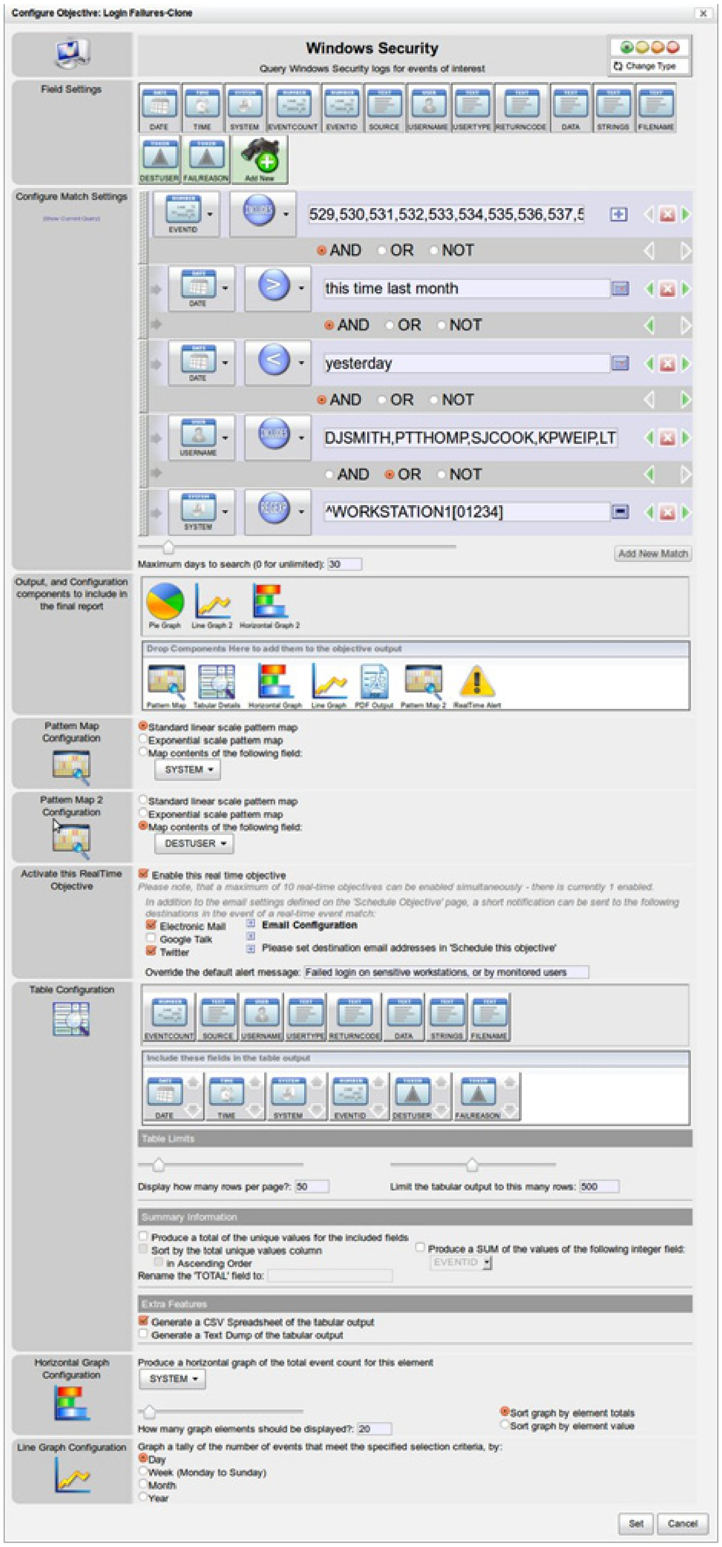
Real-time integration in every modular event-based objective means that you can receive notification of critical problems straight away.

You can even use the Snare Server's 'Token' system to break apart those big strings that tend to appear in log data, and use the resulting information in graphs, or tabular output, just like any other pre-normalized data field.

Elegant Data Presentation

Raw log data is often hard to interpret. Formatting is inconsistent, the content is esoteric, and it's hard to get your head around - particularly if it's hitting your desk at thousands of events every second

Snare receives the data, breaks it up into fields that are consistent across similar log types, and makes the data readable - with tables, graphs, and other output components that help you derive information from data, knowledge from content and results from your security strategies.



Configure Objective: Login Failures-Clone

Windows Security

Query Windows Security logs for events of interest

Configure Match Settings

EVENTID: 529,530,531,532,533,534,535,536,537,5

● AND ○ OR ○ NOT

DATE > this time last month

● AND ○ OR ○ NOT

DATE < yesterday

● AND ○ OR ○ NOT

USERNAME: DJSMITH,PTTHOMP,SJCOOK,KPWEIP,LT

○ AND ● OR ○ NOT

SYSTEM ^WORKSTATION1[01234]

Maximum days to search (0 for unlimited): 30

Output, and Configuration components to include in the final report

Drop Components Here to add them to the objective output

Pattern Map Configuration

● Standard linear scale pattern map
○ Exponential scale pattern map
○ Map contents of the following field: SYSTEM

Pattern Map 2 Configuration

○ Standard linear scale pattern map
○ Exponential scale pattern map
● Map contents of the following field: DESTUSER

Activate this RealTime Objective

☑ Enable this real time objective

Please note, that a maximum of 10 real-time objectives can be enabled simultaneously - there is currently 1 enabled.

In addition to the email settings defined on the 'Schedule Objective' page, a short notification can be sent to the following destinations in the event of a real-time event match:

☑ Electronic Mail
□ Google Talk
☑ Twitter

Email Configuration

Please set destination email addresses in 'Schedule this objective'

Override the default alert message: Failed login on sensitive workstations, or by monitored users

Table Configuration

Include these fields in the table output

Table Limits

Display how many rows per page?: 50

Limit the tabular output to this many rows: 500

Summary Information

□ Produce a total of the unique values for the included fields
□ Sort by the total unique values column
□ in Ascending Order
Rename the 'TOTAL' field to:

□ Produce a SUM of the values of the following integer field: EVENTID

Extra Features

☑ Generate a CSV Spreadsheet of the tabular output
□ Generate a Text Dump of the tabular output

Horizontal Graph Configuration

Produce a horizontal graph of the total event count for this element: SYSTEM

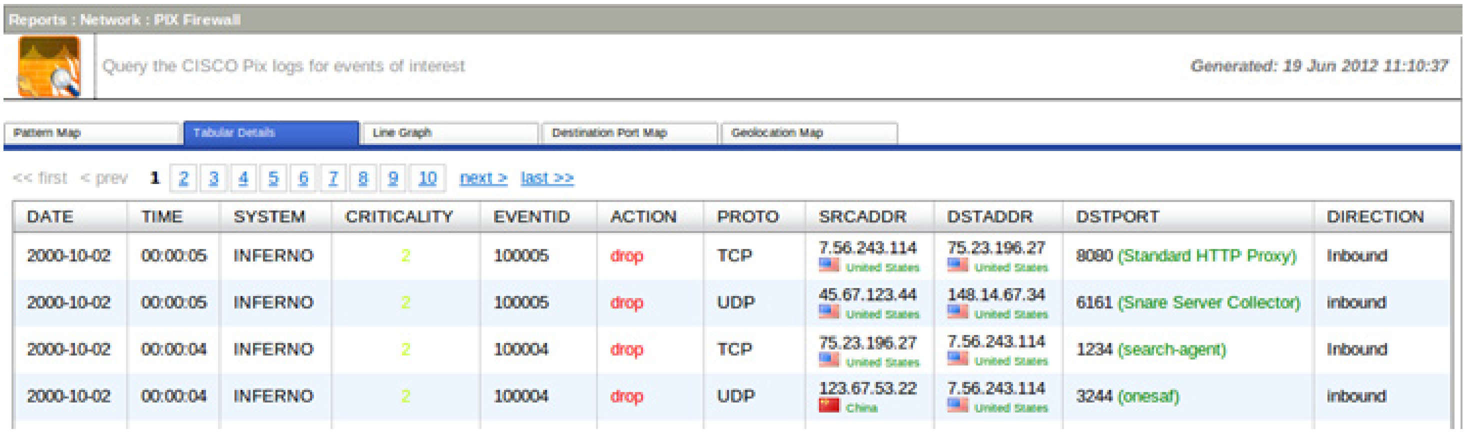
How many graph elements should be displayed?: 20

● Sort graph by element totals
○ Sort graph by element value

Line Graph Configuration

Graph a tally of the number of events that meet the specified selection criteria, by:

● Day
○ Week (Monday to Sunday)
○ Month
○ Year



Reports : Network : PIX Firewall

Query the CISCO Pix logs for events of interest

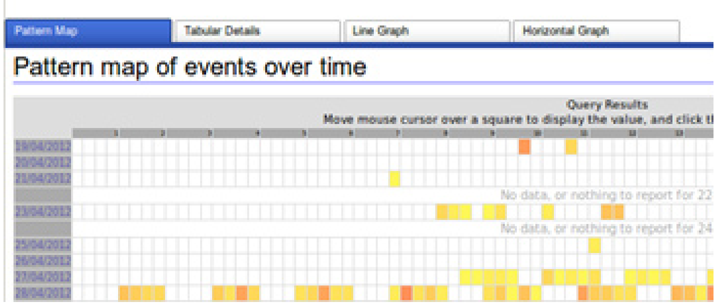
Generated: 19 Jun 2012 11:10:37

<< first < prev 1 2 3 4 5 6 7 8 9 10 next > last >>

DATE	TIME	SYSTEM	CRITICALITY	EVENTID	ACTION	PROTO	SRCADDR	DSTADDR	DSTPORT	DIRECTION
2000-10-02	00:00:05	INFERNO	2	100005	drop	TCP	7.56.243.114 United States	75.23.196.27 United States	8080 (Standard HTTP Proxy)	Inbound
2000-10-02	00:00:05	INFERNO	2	100005	drop	UDP	45.67.123.44 United States	148.14.67.34 United States	6161 (Snare Server Collector)	inbound
2000-10-02	00:00:04	INFERNO	2	100004	drop	TCP	75.23.196.27 United States	7.56.243.114 United States	1234 (search-agent)	Inbound
2000-10-02	00:00:04	INFERNO	2	100004	drop	UDP	123.67.53.22 China	7.56.243.114 United States	3244 (onesaf)	inbound

Some of the new functionality available in version 6 includes:

- Interactively sort your data by clicking on a header field.
- Jump to the first, or last page of data in a single click.
- Click on a 15 minute segment of data, and reach down into the raw events.
- Show matching query results while the report is being generated.
- A full range of additional match criteria, and output options for each and every log-related objective.



Pattern map of events over time

Query Results

Move mouse cursor over a square to display the value, and click t

No data, or nothing to report for 22

No data, or nothing to report for 24

Robust collection, and intelligent caching

Even on a low-end workstation with the lowest recommended specifications, the Snare Server is capable of collecting and storing over 10 billion events per month. Version 6.0, installed on even entry-level server hardware can triple this collection rate.

On the most common low-end commercial disk drive available at time of documentation creation (2Tb), Snare's log compression and storage subsystem can cram over a year and a half's worth of data at the rates identified above, or decades of information for organizations with less audit volume.

Snare's query response when faced with additional data, is approximately linear, which means that reports that only look at recent data, won't be speed-penalized by keeping masses of events available and ready to query on the Snare Server, and the Server is intelligent enough to cache data from reports that you use regularly - which means that the more commonly used reports, generate faster

Enabling Content

IT Security has come a long way from being the domain of a few professional specialists buried somewhere in an organizations IT cell.

Often, the people who are most interested in the security of organizational information, are those who create, and are responsible for it.

SNARE Server Version 6

The Snare Server allows you to put security reports that are uniquely tailored to your organization, into the hands of the people who are most interested in keeping the information safe, without the need to understand the intricate details of the log collection infrastructure, or the analysis engine, that supports them.

Access controls provide you with the ability to selectively provide read-only or change access to specific reports on the Snare Server, or you can send out:
* Electronic Mail
* Twitter tweets
* Jabber / Google Talk message
* PDF or HTML reports

Future Proofing your Investment

When you purchase the Snare Server and your annual maintenance subscription, you don’t just get the current version - you receive all future updates and upgrades, including access to the objective upload portal as part of your annual support agreement.

Your data is held in a non-proprietary format. If you need to export your data to another application for forensic study, we want to make sure you can. It’s your information - not ours.

The server development and support team have many decades of experience in security audit and event logs. The Snare Agents are in use around the world, and are considered by many to be the de facto standard for agent based audit log collection. The Snare Agents can be used in conjunction with other SIEM products, thought they are designed to work seamlessly with the Snare Server.

Snare’s development has always been guided directly by the commends and feature requests of our customers, and Version 6 uses these requirements as the foundation for a robust, comprehensive security event management system.

Flexible Licensing

With Version 6, Intersect Alliance has also introduced new licensing types to accommodate any budget. Snare, in the past was provided as a perpetual license, however term licensing and subscription based licensing have been introduced.

Term based licensing provides for slightly lower upfront cost, as well as lower on-going cost, and subscription based with a three year contract.

For more information, contact your SNARE Server Sales Representative
snaresales@symtrex.com | 1-866-431-8972

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com

symtrex inc.
Network Security Specialists

Who’s Watching Your Network?