SECNOLOGY

SECNOLOGY

THE SECURITY BIG DATA MINING COMPANY

www.secnology.com

SUMMARY

1. Core Modules

2. Additional Modules

SECMANAGE

What Makes the SECNOLOGY Data Mining Platform so Powerful?

The heart of the SECNOLOGY architecture is SECmanage, which performs numerous operations on all events in real-time, on demand and on schedule. Two significant technological advantages make SECNOLOGY the most powerful Data Mining solution available today, able to process Terabytes a day faster than anyone.

TECHNOLOGICAL ADVANTAGES

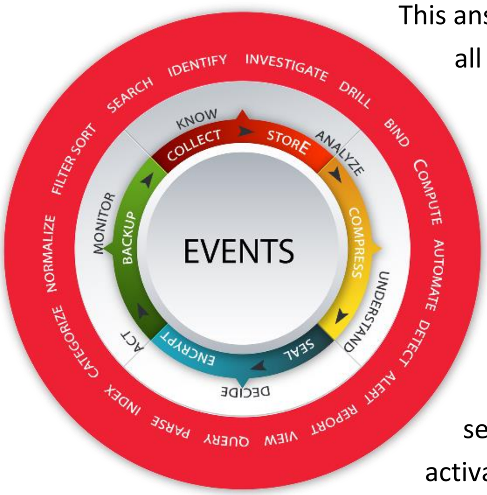
GRID COMPUTING ARCHITECTURE

Using a flexible Grid Computing Architecture to provide power, scalability and high-availability, SECmanage can process data on many SECmanage systems simultaneously. To process 17 Terabytes a day, simply position multiple SECmanage systems. Leveraging this Architecture, dedicate some SECmanage systems for specific tasks such as reporting, correlating, binding, alerting, archiving, parsing, etc…

TURBO INDEXING METHODOLOGY

Leveraging our patented STIM to avoid using a database makes SECmanage the most powerful event management solution available on the market. By not using a database, SECmanage frees the Architecture from the underlying complexities of event analysis and provides a simple, ergonomic and effective tool. In terms of analysis speed, it outperforms all its competitors on identical platforms 100 to 3000 times!

How Does SECNOLOGY Turn Data Events Into Actions?



This answer is in two parts. First, decision makers need a single standard view of all the information received from network and security devices managed. Use SECmanage to create business specific Dashboards and numerous customizable Reports from a single source or from multiple sources as needed. The insight derived from the Dashboards and the Reports provides the first part of the answer.

The second part is due to a number of advanced features available in scheduled or event driven Jobs. Jobs can use a predefined set of Rules to watch, observe and analyze events and then conditionally trigger a sequence of Actions to execute. A Rule is a set of triggers that, once activated, launch a predefined set of Actions. Actions may occur simultaneously and may run external 3rd party applications, such as applying a configuration change to a Firewall or comparing a change to a critical server.

hese combined features will help you turn event data into actions.

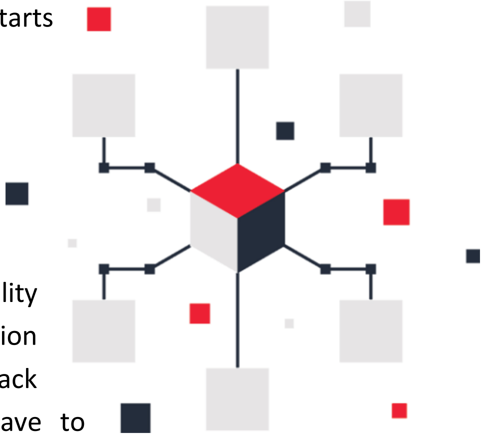
Powerful and flexible Features

- Detect anomalies
- Normalize data events
- Filter data events
- Search and explore data and events
- Correlate data events from multiple sources
- Compare different metrics
- Process jobs and alerts
- Create Graphs and Charts
- Monitor the global environment in real-time
- Investigate after an incident
- Parse events and traces
- Segregate data events
- Categorize data events
- Enrich data events
- Evaluate triggers and measure thresholds
- Process data events
- Manage the Life Cycle of data events
- Provide dashboards
- Generate Reports in real-time
- Record all the traces of all actions

SECCOLLECT

How Do I Get continuous Visibility ?

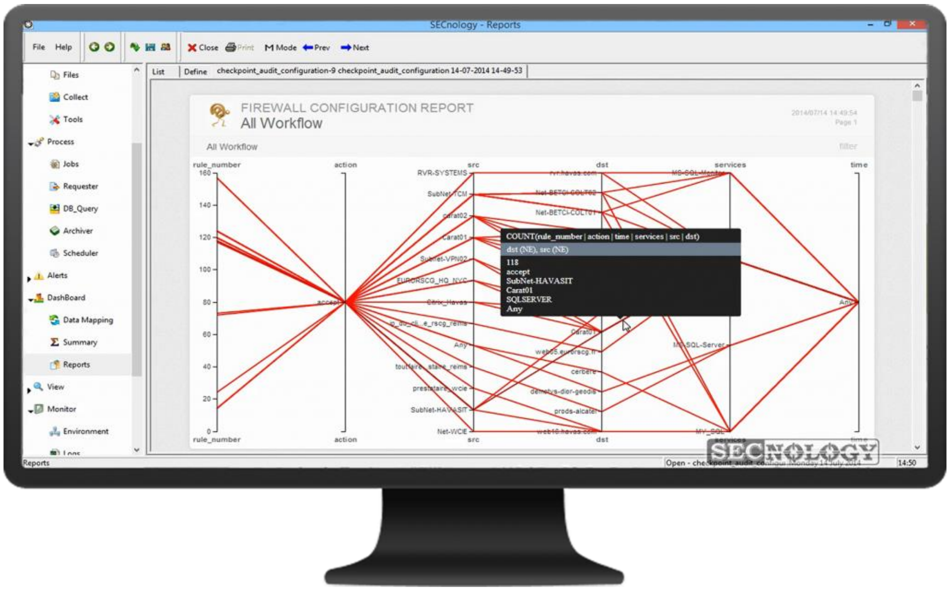
How do I get continuous visibility so i can understand where the vulnerabilties are and take corrective action in a timely Manner?Do you need an answer to this question? SECNOLOGY provides a comprehensive solution to this challenge, and the answer starts here. The first step is to gather network & security events.



GATHER YOUR SECURITY EVENTS

The first thing to do when you want to acquire continuous visibility to improve your network security is to collect all the information needed. Why? Just imagine that your IDS has detected an attack against one of your servers. The security manager will have to investigate many different events generated by numerous devices: routers, firewalls, gateways, etc… to see if there is a hidden clue regarding this attack.

The challenge is that this information is everywhere since all network and security devices generate their own event data, potentially creating gigabytes of data in a short time.



SECnology - Reports

checkpoint_audit_configuration-9 checkpoint_audit_configuration 14-07-2014 14-49-53

FIREWALL CONFIGURATION REPORT
All Workflow

2014/07/14 14:49:54
Page 1

All Workflow

COUNT(rule_number | action | time | services | src | dst)
dst (NE), src (NE)
118
accept
SubNet-HAVASIT
Carat01
SQLSERVER
Any

Collect Events in Real-Time

With SECcollect, SECNOLOGY can collect a large number of events directly from devices, registry or files in real time, on events or on demand. SECcollect can manage all types of formats, including those from custom in-house applications, without the need for developers or toolkits. Store data centrally and/or remotely, archive and secure the data according to policy, and automatically manage the whole data life cycle, including availability, accessibility, integrity, confidentiality, segregation, period retention and purging, in accordance with your policies.

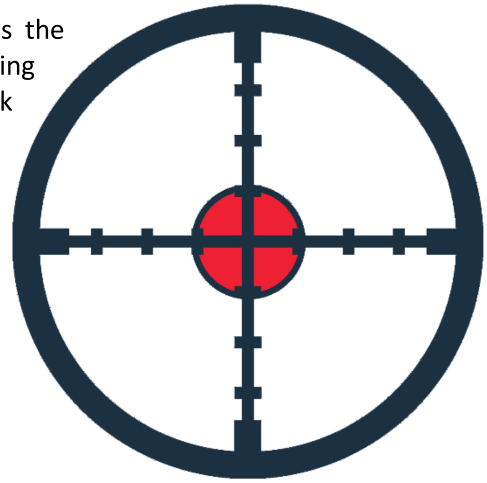
How SECcollect is not intrusive ?

SECcollect is not intrusive and can collect data in real-time from a large number of devices simultaneously using a many standard protocols: UDP, TCP, SSL, SNMP, POP3, CIDEE, SDEE, NetFlow, jFlow, sFlow, MS-EVENTS and LEA OPSEC. Because of its multi-threading and multi-processing architecture, SECcollect can process hundreds of thousands of events per second.

SECcollect does not have to parse, normalize and store the data in a database. This advantage makes SECcollect able to outperform all its competitors with an unprecedented level of performance. SECcollect listens only to authenticated sources and writes the data in standard flat files in contiguous sectors as raw data, filtered data or both at the same time.

SECAGENT

When Do I Need SECagent?



The short answer is that the SECagent is not required unless the system or device you need to monitor is unable to send events using one of the numerous protocols typically used by network management platforms. Most network and security devices as well as Linux/Unix systems are typically able to send events; however, most other environments are not. If one of these protocols is available to send events, then SECcollector is able to receive these real-time events directly. Otherwise, SECagent is needed.

ACTIVELY RETRIEVE EVENTS

SECagent actively captures event data from systems that cannot send it, which ensures that real-time analysis is complete and comprehensive. This is an important issue for most organizations because not all systems and devices on the network are able to send their event data to either a central or a distributed repository on their own. While some systems and devices can send events to a predetermined location on the network, there are many which cannot fulfill this requirement. This can create an important hole in a comprehensive network infrastructure and security management system. To assess fully the state of the network for the systems and devices deployed all event data must be available and fully analyzed.

SECagent fills this gap and is able to get event data from sources that are unable to send them. It will fetch, watch, pull, and send this data to SECcollect on the fly. SECagent is able to watch file systems, Windows events, data files, folders, registry keys and Active Directory events.

This product ensures that all events, whatever the platform, are available for a comprehensive network infrastructure and security management real-time analysis as well as for retrospective analysis.

SECagent can:

- Manage and control file and folder integrity
- Manage user rights and access privileges on files and folders
- Audit in real-time user activity on targeted files and folders
- Audit in real-time access and changes to Active Directory

With SECagent Find:

- All the systems to which a specific user is connected
- The users who connected to a specific system in a certain time frame
- All the changes that occurred to group members in Active Directory
- The changes in users accounts
- All read access to a file or group of files on a critical server

File Integrity Management

Any event related to adding, changing or deleting a file, a group of files, a folder, a group of folders or even a security or network device configuration is immediately captured by SECagent and forwarded in real-time to SECcollect. SECmanage also provides file integrity management independently.

The combination of both SECagent and SECmanage guaranties the integrity of a remote target by detecting any change on that target and triggering automatic recovery of that target. Whatever the change, enforce the reference image in production.

LDAP and AD Audit and Real-Time Monitoring

Use SECagent's advanced features to monitor all operations affecting Active Director or LDAP.

SECagent performs real-time monitoring in many situations, tracking:

- All the systems to which a user connects
- The users who connect to a specific system
- The changes applied to a group in Active Directory
- All the changes applied to Active Directory objects
- All the changes applied to Active Directory services
- The changes applied to user accounts in Active Directory

A good example is a Web site. Should you decide to protect your Web site by keeping an image of the site as a reference somewhere on the network. Then, in case of any change to the Web site, SECNOLOGY will automatically detect the change and restore the site using the reference. This will not protect your web site from attack, but it will definitely prevent the Web site from being corrupted!

SECweb

Provide Access to SECNOLOGY to a Web Browser

SECweb is a Web Portal allowing authorized users to access their personal SECNOLOGY environment using a web browser. The SECNOLOGY Administrator defines the jobs, reports and alerts that are available and validates the SECweb environment for each user. These users can then access the available jobs, reports and alerts and can create personalized jobs based on these by simply using a web browser, i.e.: Internet Explorer, Firefox, Chrome, etc… With an easy to use web interface, the user is able to select his events and jobs, to upload events to the portal, to run jobs on selected targets and to access his dashboards, reports, alerts and files.

A User-Friendly Web Interface

The objective on SECweb is to make the user experience the easiest possible while maintaining a rich feature set. The SECweb user is able to use the most critical components in SECNOLOGY simply by pointing and clicking. The user-friendly interface gives complete access to SECNOLOGY functionality while protecting the SECNOLOGY configuration.

Complete Reports

The reports available to Web Browser users are complete SECNOLOGY Reports. These reports can be from a single source, for instance Juniper events, or from multiple sources including, but not limited to, Check Point, Cisco, IBM, and Microsoft events. Every SECweb user has a private and secure storage area, and all the rights and privileges in that space to create, move and delete files and folders as needed. The SECweb user may also save his reports on local storage.

Power and Safety Combined

Since SECNOLOGY is running behind SECweb, the user can access all the power made available by the SECNOLOGY Administrator, but cannot modify the system’s configuration.

The SECweb user can manage all types of events whether they are real-time or historical. Data to process may come on the fly or may already reside somewhere on the network in flat files or in existing databases. The SECweb user can easily search, filter, analyze, classify, organize, normalize and tag data for forensics investigation. He can perform user activity tracking, compliance monitoring, trouble shooting, risk mitigation, incident response, specific event detection and much more in a very easy and flexible way. With all this power, the SECweb user can generate metrics, control thresholds, generate actionable alerts and notifications, generate automatic reports and dashboards, view charts and graphs, use different ways to cross correlate heterogeneous data and turn raw data into clear business information.

SECreport

Customized Reports

The reporting tools included in today's event management platforms are more and more powerful and provide administrators not only with a birds-eye view of occurring events, but also make it possible to take a deeper look into IT processes. SECreport meets these expectations.

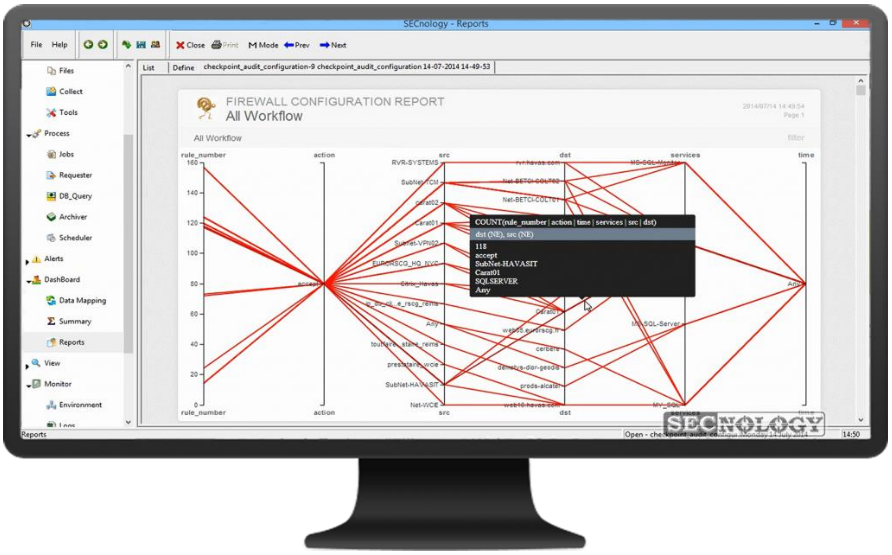
Automatic Reports

Combined with the power of the SECalert and the SECprocess modules, you can achieve incredible results with SECreport. Having defined a set of alerts and processes that address your specific IT environment's requirements, SECNOLOGY can get you the results automatically.

The SECreport module is a standard feature of the SECNOLOGY Platform.

How to create a report ?

SECreport provides a number of standard reports that are customizable to create extensive and easy to understand reports. Based on your events, these reports may be stored in either HTML or PDF formats.



FIREWALL CONFIGURATION REPORT
All Workflow

COUNT(rule_number | action | time | services | src | dst)
dst (NE), src (NE)
118
accept
SubNet-HAVASIT
Carat01
SQLSERVER
Any

SECjob

Industrialize Operational Intelligence

The SECjob module was added to the SECNOLOGY Platform to industrialize operational activities and eliminate this problem. Any process defined within the SECNOLOGY platform can be industrialized and automated. If human intervention is required, alerts can be sent. But if the response to an event does not require human intervention, then the actions required in response to the event can be fully automated, fully industrialized.

How Does SECNOLOGY Turn Data Events Into Actions?

This answer is in two parts. First, decision makers need a single standard view of all the information received from network and security devices managed. Use SECmanage to create business specific Dashboards and numerous customizable Reports from a single source or from multiple sources as needed. The insight derived from the Dashboards and the Reports provides the first part of the answer.

The second part is due to a number of advanced features available in scheduled or event driven Jobs. Jobs can use a predefined set of Rules to watch, observe and analyze events and then conditionally trigger a sequence of Actions to execute. A Rule is a set of triggers that, once activated, launch a predefined set of Actions. Actions may occur simultaneously and may run external 3rd party applications, such as applying a configuration change to a Firewall or comparing a change to a critical server.

These combined features will help you turn event data into actions.

Do you need automate certain responses ?

For immediate action in response to an event that does not require human intervention, then SECprocess can leverage SECjob to automate the actions required in response to the event.

The SECjob module is a standard feature of the SECNOLOGY Platform.

SECalert

A Fast Response Time

Response time to an occurring event can be critical, especially for certain events!
SECalert was designed to reduce event response time to zero! Whenever SECNOLOGY is running (i.e.: building graphs, collecting events, etc…), whether in interactive mode or in Job mode, SECalert watches over the processes and analyses them based on a predefined set of triggers. When a match occurs, a predefined action or a sequence of actions is executed or Administrator is prompted to make a decision concerning the event.
With SECalert you will never miss an event and can be reassured that you will be alerted should a suspicious or dangerous event occur anywhere in your environment!

Define Rules

When SECprocess analyses an event, in interactive or batch mode, a predefined set of rules watch, observe and analyze the process and will conditionally trigger a sequence of actions to execute. A Rule is a set of triggers that, once activated, launch a predefined set of actions.

The rules are easily customized as needed.

Automate Actions

Actions may occur simultaneously and may run external 3rd party applications, such as applying a configuration change to a Firewall or comparing a change to a critical server.
Six types of actions are available in SECalert, enabling a wide range of responses to any event:

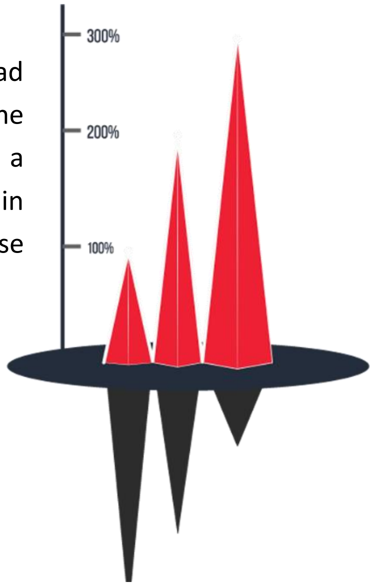
- Send emails to one or more destinations, with attachments if needed.
- Send a Net Send command to an IP address or to a sub network in broadcast mode.
- Display a Pop-Up message
- Write a script or a sequence of commands to a batch file
- Create a file fed with dynamic parameters
- Trace the alert in transparent mode
- The SECalert module is a standard feature of the SECNOLOGY Platform

How to never miss an event ?

With SECalert, you will never miss an event and can be reassured that you will be alerted should a suspicious or dangerous event occur anywhere in your environment!

SECview

Visual Data Mining Technology



As an advanced Big Data Mining platform, SECNOLOGY's power and flexibility lead by example. A major advantage comes from the Visual Data Mining interface in the SECview module. Display Event correlation using SECview to show exactly how a situation evolved in detail. This is possible for either a specific range of time and in real-time and allows the selection of any of the available variables, whether these are Fields, MetaFields or any combination of multiple data sources.

To enhance visibility, use the graphical zooming feature to dynamically adjust the time frame to analyze.

Find "The Event" in an Ocean of Events

SECview is a multidimensional real-time cross data graphical monitoring tool that provides a global view of what is happening across the network, servers and/or applications. Leverage SECview's power to easily track the behavior of your IT assets.

View and compare the evolution of many variables simultaneously, and correlate them with the "normal" standard reference behavior expected. The events are shown in a detailed or an aggregated format and the zoom feature provides visual real-time evolution of a specific event variable.A symbol of varied size and color represents every data flow or group of data flows in the monitored environment. The size property of a symbol can be defined to represent the type of information. The color of the symbol can be customized to represent quality control information relevant to a set of devices in your IT environment.

Quickly see the important event in an ocean of similar ones. Instantly notice abnormal behavior and take appropriate action for deeper investigation into the origins of the anomaly.

Business Line Views

Set “business line views” to provide a transverse, cross device view based on specific criteria. For instance, to see the number of current open sessions on each device for a specific link (router, firewall, proxy, anti-virus, switch, server, database, etc…). Create a real-time view that will display the CPU usage on a set of devices in the DMZ or a view for all the IP addresses that are seen by another set of devices. The possibilities are endless.

SECmonitor

Easily Supervise your Entire Infrastructure

In order to supervise all the systems within your infrastructure, including all network and security devices, it is critical to see everything that is happening in your environment at all times. Only tracking some devices periodically will lead to both performance issues and security breaches.

The ability to monitor the entire corporate IT environment enables an enterprise to be more effective, more efficient and ultimately more secure. SECmonitor provides this insight.

SECmonitor tracks the status and provides the historical details of all that SECNOLOGY is doing in your IT environment by combining the output of all SECNOLOGY modules into a single easy-to-use tool. Simply put, SECmonitor provides a visual status of the complete IT Environment that SECNOLOGY is supervising. As you look at each SECmonitor section, it will show the status for each element defined in that section and give the ability to access a detailed history of the activity for each element in that module.

The SECmonitor module is a standard feature of the SECNOLOGY Platform.

SECMONITOR SECTIONS

ENVIRONMENT

The Environment module is where all corporate network and security devices, applications, and gateways as wel as SECNOLOGY collectors are defined.
This SECmonitor section provides the status of all the components defined in your IT environment. Immediately notice if an element is Up or not.

LOGS

The Logs module is not only where all event traces are located, but it is also where parser definitions, signatures and numerous other tools are either defined or implemented.
With SECmonitor, instantly see if these are running or idle in the indexed status screen and find details of all activities in the history tab.

PROCESS

The Process module is where all SECNOLOGY processes, including jobs and data lifecycle management features, are defined and scheduled.
This SECmonitor section shows the status and provides a history of all activity in the Process module. It enables you to monitor the tasks in progress as well as all the work yet to be treated or already treated.

VIEW

The View module is a powerful Visual Data Mining tool used to graphically display event correlation to show exactly how a situation evolved in detail.
This SECmonitor section provides the status and history of the view module.

DASHBOAR

The Dashboard module allows you to create customized reports, but it also provides several features to transform raw data into simple, accessible and meaningful information without compromising event data integrity. This increases the readability of reports.
This SECmonitor section indexes the status and history of all Dashboard activity.

ALERTS

The ability to respond automatically to events in real-time is a powerful feature in SECNOLOGY. The Alerts module's primary function is to define the rules that will conditionally trigger a sequence of actions, including alerts.
This SECmonitor section provides an overview of all the defined rules. It lets you know at a glance if a rule is active and provides details of all activity showing the status and history of all Alerts.

THE SECURITY BIG DATA MINING COMPANY

Core Modules

SECMANAGE

SECCOLLECT

SECAGENT

SECWEB

Additional Modules

SECREPORT

SECJOB

SECALERT

SECVIEW

SECMONITOR

WWW.SECNOLOGY.COM

El Granada CA 94018, USA ☎ (415)-762-1820 ✉ sales@secnology.com