GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Evaluation of Central Event Logging, Monitoring & Correlation Tools – Master Platform Red Hat

The three pillars of security:

Confidentiality
Integrity
Availability

Submitted By: Magdalena Hewryk
Date: Nov 2, 2004
GSEC Practical v1.4c, Option 1

© SANS Institute 2005, Author retains full rights

© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract

There is a wide variety of Security Correlation tools available, from appliances through network based and host based products. There are commercial and freeware software. I did the search based on suitable technology and tools to support cross platform logging correlation covering UNIX/Windows and Network devices (UNIX/Linux, MS, switches, IDS, FW). I was concentrating on commercial software product which support RedHat Linux platform for the Master Server. Particularly I was concentrating on RH ES 3.0 for Server platform. My choice was based on Linux/UNIX security and stability over Windows platform, more flexible maintenance (applying patches, fixes) and above all better

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005, Author retains full rights.

performance with RH than Win Platform. High Availability, clustering, robustness were the important factor when choosing the platform as well.
For hardware I have chosen IBM xSeries 345 servers with dual processors and max RAM. I was open for database option. For storage I decided to use SAN – and calculated to use 600 GB archived data per year when correlating 125 devices logs, no more than 15 million events per day.

The central logging facilities was going to analyze and report on significant security events and trends. It would address a number of critical client, audit and legal compliance requirements.

Conditions to pick the product were low price for high value, the product was not going to have the security analyst at the console 7x24, event rules, conditions would not be maintained on 7x24 hour basis, no need for ongoing threat modeling.

What is the security event logging and correlation tool

The tool should allow to monitor the whole IT environment (UNIX/WIN/Network devices) and manage current security status, based on auditors requirements from a centralized location in real time. The purpose is to take quick action and provide appropriate reports in a timely manner.

By collecting all systems events, merging them, centralize them the Security department can provide a real time view into a network's security status, enabling a proactive approach to security within a company. Through automated alerts, by creating thresholds, rules, alarms the security can be monitored and reports about the security events across

Finally I was looking for a product which was able to trace **W7** – Who, What, When, Where, Where from, Where to on What. When using a search I should be able to provide either userID or IP and the program should scan through all correlated logs and give me not only the output with the search pattern but also analyze it according to security standards/knowledge and rules.

To protect against downtime and loss of confidential data the product has to have the extensive notification capabilities and have a security knowledge built in and be capable to expend it.

The key benefits include the ability to meet legal and business log-retention requirements. I was looking for compliance with SOX, GLBA, CASB 1386. In addition to ensure security audit policies are enforced across organization by centralized definition and enforcement of audit setting that should be set and

© SANS Institute 2005 Author retains full rights.

enforced across all workstations and servers. The only way to prove it is through centralization of service activity, logons and other events.

The summarize the objectives are to capture log data for analysis from UNIX/Linux, MS, routers, switches, IDS, FW and provide reporting functionality for security analysts. The products should provide the capability to analyze normalized data when an event occurs and correlate information to minimize event notification.

Infrastructure without any security correlation tools

- If there is no centralization of the event logging and monitoring in the company
- If each group Network/Intel /UNIX either has its own centralized system or lacks for the monitoring their system logs for the security purpose.
- If there is no cross platform tool to merge all logging information
- If a security department/analysts cannot view and monitor systems events on the regular basis

Business Enterprise Needs & Drivers

- Ability to filter, aggregate and correlate logging data across platforms (UNIX/Intel/Network)
- Real time security monitoring and historical analysis
- The security reports integration for regulatory and audit compliance
- Consistent and continuous classification of intrusion attempts
- No appliances
- UNIX platform (RH) for Master preferred due to license cost

- ❖ Event Correlation – consolidate/analyze related events
- ❖ Centralized Management – by helpdesk, operations, etc
- ❖ Scalability – network might growth
- ❖ Extensibility – IDS, vulnerability scanners, etc
- ❖ Portability - not to be stuck with a specific platform

Logs Correlation	Must have
Security Audits	Must have
Real-time Monitoring	Must have
Archive and Data Mining	Must have
Reports, Visualization,	Must have

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Notification

Database Capacity

The table below demonstrates the storage based on the network which creates/captures 15 millions events per day (via SYSLOG & Windows logs). That includes UNIX, Win and Network devices logs.

Online Database	
1 million events (4K per event)	4 GB
15 million events per **day**	60 GB
Event Value Archive - Raw log data compression 10:1 or 20:1	
1 million events	200 MB
450 million events **per month** (15 millions x 30)	100 GB **monthly**

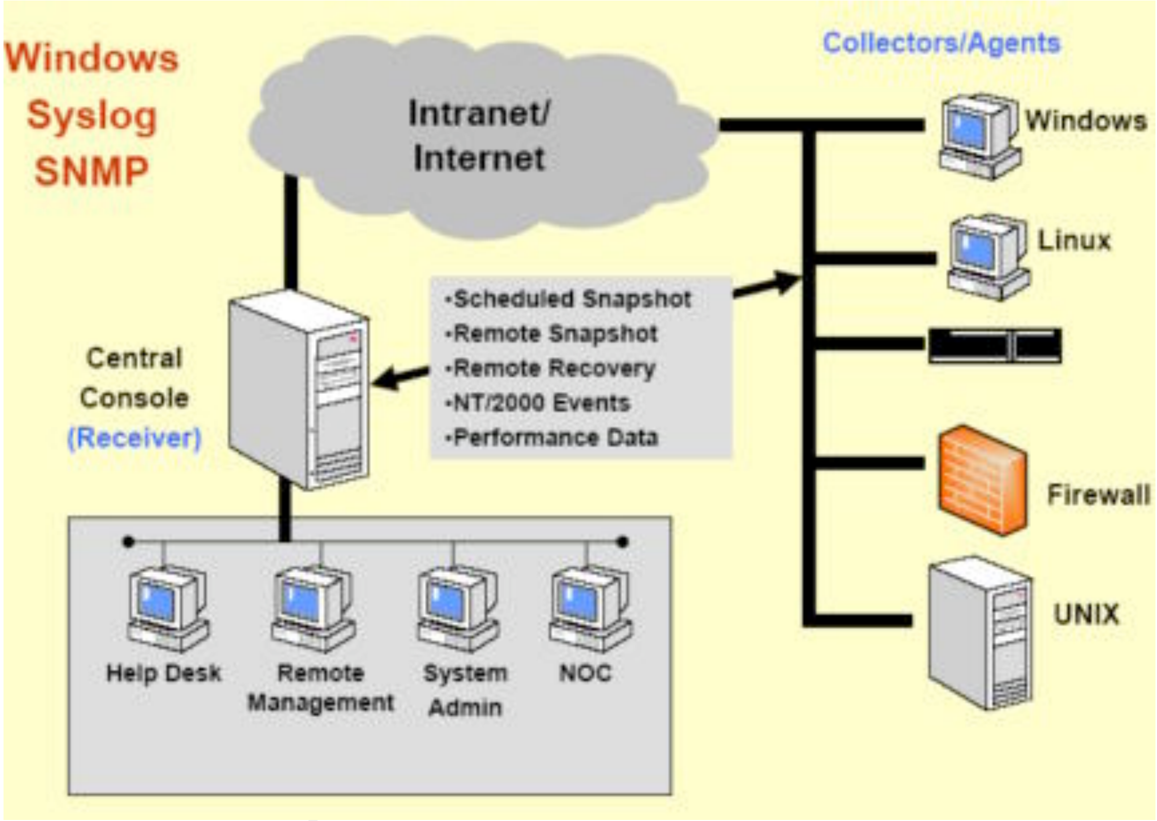
Typically, the number of events logged or alarms raised can be enormous. It leads to deluge of information. However the data needs to be kept and archived for at least 6 months. It will give 600GB in total. Data stored in the database can be replayed back into the product. All products give users the capability to replay information retrieved in a report. For example an analyst can query user activity for the past two months, and replay the results into SIM to re-create correlated conclusions and visualizations of the user's potentially damaging activity. Keeping historical database off-line and compressed is one of the most important feature for logging correlation products. SIM products should permits replay of historical data, even while they are processing real-time data.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Detection and Reaction

[1]



The Event Logging and Correlation Product should support the following functions:

Log Consolidation: Event Consolidation should consolidate events from Windows, UNIX and network devices. The event consolidation process has to be reliable (no data compromised), timely (real time) and non-intrusive (ideally agentless option). All events should be consolidated into a common database supported by Software and hardware platform.

Reporting: Once events are consolidated into a database, they are ready to be analyzed and the business reports can be produced. The ability to search the database on any criteria and generate the required report is key for any analysis. The pattern of events, rules and actions

[1] Prism Microsystems. Total Event Management.

© SANS Institute 2005 Author retains full rights.

should be pre-defined. I was looking for a product with predefined reports and knowledge base. A baseline of security event behaviors to be easily established to shorten the window of vulnerability. Ability to classify intrusion attempts and to track use id's and IP address via logs are essential for event tracking. To link those events by identifying source across multiple devise and to set thresholds and triggers for custom actions is a must.

Log Aggregation: Most products support MySQL, Oracle or its own database. The non-RDBMS database can be query able when compressed. Compression can be on a raw log data in 10:1 or 20:1 ratio. The ability to query for historical events and data mining as well as track real time events is crucial for analyzing the event. Archiving saves tones of space on SAN. Bringing database online, offline easily is another factor to keep in mind. Space is a very important factor when evaluation security event correlation product because of the number of events going through the network. So space, archiving and compressing database needs to be kept in mind when looking for the product.

Presentation: The visualization via dashboard, workstation console or web browser needs to be provided. The visualization capability allows to identify anomalies quickly and drill down to the root cause of the anomaly. I learned that there is generally different price for workstation console and web browser view so the differences for workstation and web access needs to be understand before deciding how many console licenses need to be bought.

Role Base Permission: Every part of the application should relate to Access Control. Depending on logon credentials the user will have a completely different view of the product and read and write privileges will be limited accordingly. The Help Desk or Operations or Security Analyst they can have access to the application on the role base permissions.

Intrusion Prevention: Ability to receive data from Vulnerability Scanner products such as Nessus, Internet Scanner, eEye Digital Retina or IDS will allow to determine the risk assessment Automatic responses like the following should be included: automatic creation of a trouble ticket, disabling a user account, shutting down a service, shutting down a machine, blocking an Ip address , resetting TCP/OP communication, launching automated vulnerability scans of attacked hosts

© SANS Institute 2005 Author retains full rights.

Tools Evaluation Criteria

Below is the table with the criteria base on following. I tried to cover all criteria making sure the products is capable of doing the basic functions like reading from all logs which are required (Win/UNIX/Network, special databases, Lotus Notes), it meets Five drivers like real time correlation, data mining, compression, filtering. Then I evaluated the capacity of intelligence of the product. Can the product discover the network or does it have the ability to learn if the event happened in the past ? We call it intelligence data discovery feature. The log analysis, tracking user policy violation who what, when , where on what and from where, where to should be in available from the product as well. Permissions, role based access to see the events, customization, functionality and technology needs need to be address.

- ❑ Basic information
- ❑ Top Five Business Needs & Drivers
- ❑ Log Analysis
- ❑ Viability and Intelligence of the Product
- ❑ Features
- ❑ Technology and Functionality

I've conducted phone interview with the Top Players recommended by Maic Quardrant for IT Security Management, 1H04. In addition I went through the White Papers for information on each product . The table gives a references what each product was capable of. I was concentrating of looking on intelligence of the product, not just correlation of events but also self determination of the problem, ability to learn from the history. I was looking for minimum adjustment, configuration after installation and more out-of-the-box solution.

Evaluation Criteria	**Perquisites for The Cross Platform Central Event Logs Correlation**	**NSM/ Intellitactics**	**ArcSight**	**New SECURE/ Guarded Net**	**Security Threat Manager/Open Service**	**SenSage /Addamark**
Basic Criteria	Evaluation Period – How many days for testing pilot is provided?	30 days	30 days	30 days	30 days	30 days
	Master Server installation platform: UNIX/WINDOWS/APPLIANCES OS details	Harden RH 9 Advanced Function, Data Acquisition, Remote Console	RH ES 3, AIX, Solaris, Win/Mac	RH ES 3/Solaris	Solaris/RH 9/Win	RE ES 3

© SANS Institute 2005 Author retains full rights.

	Client/Server Architecture? Separate agent installed on the client? Client OS supported platform	Yes	Yes Syslog or Windows Smart Agents	No agent required	Yes	Yes Collectors Linux PC, Scalable Log, Analyzer Windows
	Host-base or network-based product	Yes	Yes	N/A	Yes	Yes
	Specific names of logs the product can generate the security events. Sources: 1 Windows NT, 2000, or XP event logs maintained on each Windows server 2. Syslog created by UNIX systems 3. Proprietary audit logs from AIX, SUN, HP-UX 4. W3C log from Web servers such as Apache, iPlanet and IHS 5. SMF records from OS/390 6. Oracle activity logs maintained by Oracle tables 7. Dimino logs kept in Lotus Notes database 8. Syslog or SNMP traps from firewalls, network devices 9. Logs from intrusion detection software typically generated as SNMP traps	Yes except 5 & 7	Yes – ALL	Yes except 5&7	Yes expect 4 &5& 7	Yes except 7
Top Five Business Needs & Drivers	Ability to filter, aggregate and correlate logging data across platforms in a simple, accessible reporting system and dashboard displaying form	Yes Very strong features	Yes	Yes	Yes	Yes Drill down, graph
	Real time security monitoring . Generates a real-time overview of IT security across the platforms	Yes	Yes	Yes	Yes	Yes
	Archiving audit data for later after-the-fact investigation. Data Mining, Data Discovery	10:1 or 20:1 compression	Yes Up to 20: 1 compression	Yes	Yes	10:1 compression
	Integration of the security reports for regulatory and audit compliance	Yes – 100 different predefined web based reports	250 out-of-the-box reports	Yes Number of pre-built reports	Yes	Ovr 100 out-of-the-box reports
	Can function as host-based IDS or can function with other IDS? Integration with the HostBased ID?	Not IDS	Not IDS	Not IDS	Not IDS	Not IDS

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Log Analysis	Monitoring and analyzing both user and system activities. Based on UserID or HostID?	Yes	Yes	Yes	Yes	Yes Atgranular level
	Tracking user policy violations: Who, What, When, Where, On What, From Where, Where to	Yes – out of the box	Yes Rules can be easily written to track policy violations	No	As defined by customer	Yes – pre0buit reports
	Recognizing patterns of typical attacks. Integration with Nessus?	Yes	Yes – smart Agent for Nessus	Yes	Yes	Yes i.e., port scans
	Analyzing abnormal activity patterns	Yes	Yes TruTreat Discovery Engine	Yes	Yes	Yes I have to teach a product that something happend
	Assessing system and file integrity	Yes with 3rd party devices	Yes, with Tripwire	No	Ys	Yes Includes reports on file modifications and attempts to access files
	Analyzing system configurations and vulnerabilities	With Nessus or ISS, Foundstone	With Nessus or Internet Scanner, eEye digital Retina, etc	No	Yes	With vulnerability scanner logs
Viability/ **Intelligence**	Heterogeneous sources - will need to obtain information from listed platforms & from all host in range IP addresses as well as work with list of hosts and IP addresses. The key word is a network topology discovery ability	No	Yes – based on RFC 1918 addressing	No	Yes by CIDR block	No discovering Stores all Ips and can produce reports on IP ranges
	Integrity management - will need to be able to verify the integrity of the data which is stored in the logs - if the data is not compromised when moving to the central cross platform location	Yes	Yes	Yes	Yes	Yes
	Time stamps on servers must be synchronized. Determine the time interval	Yes	Yes	Yes	Yes	Yes

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

	tool					
	Historical analysis - ability to learn if the event happened in the past - set filters in the event viewer to capture past events, store events, trend-capturing capability	Yes	Yes Active Channels can be set to go back as far as retention period	Yes	Yes	Yes Its own database Non-RDBMS 10:1 (raw logs) 1/40th of a traditional RDBMS. All compressed log data is query-able.
	Determine the time interval between specific events as a troubleshooting tool	yes	Yes	Yes	Yes	Yes
	Visualization - ability to annotate the event log - to refer to Service Centre notes and quickly solve the recurring problem by suing the solution	Yes Create ticket based alert	Yes Dashboards and TruTreats Discovery Engine	Yes	Yes Runbook can be incorporated into console	Yes Knowledge base integration and annotations
Features	Provide continuous classification of events real time, multiple feeds from different servers/databases	Yes	Yes	Yes	Yes	Yes
	Automation the incident-response capability. Managing security incidents	Yes Email, pager alerts, screen	Yes	Yes	Yes	Yes
	Monitor Users attempting to access secured shares and confidential files. Tracking activity that affects sensitive data, documents and transactions	Yes	Yes with IDS	Yes	Yes	Pre-built insider abuse detection reports (access of sensitive data)
	Detect attacks using local user accounts. Tracking activity of authorized users.	Yes	Yes with IDS	Yes	Yes	Pre-built reports (invalid attempts, unauthorized access)
	Create alerts for specific events and conditions occurring on the network	Yes	Yes	Yes	Yes	Yes
	Easy filtering and analysis of important events	Yes Pre-packaged rules (drag and drop)	Yes	Yes	Yes	Yes drill downs

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

	Provide continuous classification of intrusion attempts	Yes	Yes Provide to write follow up rules that reference these active lists	Yes	Yes	Yes
	Provide continuous classification and follow-up of events . Provide the ability to interpret security log data	Yes	Yes	Yes	Yes	Yes No knowledge base built
	Thresholds setup, triggers customization.	Yes	Yes	yes	Yes	Yes
Technology	Operating system: RH, AIX, Solaris	Harden RH 9	RH ES3, AIX, Solaris, Win, Mac	Solaris or RH ES 3	Yes all	Linux cluster RH ES 3
	Single Point of Failure – Failover, Cluster	HA failover or clustering on OS level	Via Veritas and Legato Cluster Agents can send data to multiple managers	Load balancing option	Multiple correlators and consoles deployable in tandem	Linux cluster RH ES 3
	Hardware requirements: SUN, IBM, Intel RAM, CPU multi-processor threaded, I/O, Disks Scalability	Advanced Function and Data Acquisition servers: 6 GB RAM, dual 3 GHz CPU Remote Console: 1.4 GHz CPU 2 GB RAM Grahic card 64MG RAM	Dual CPU Depends of req.	Depends how many events per second	4 GB RAM, dual 1GHz CPUs	Dual 3.2GHz CPU 3.4 GB RAM
	Database: Oracle/DB2/MYSQL	Own database or Oralce	Oracle or DB2 – license separate	Oracle & MySQL	MySQL	Own non-DBMS Raw log data stored at a 10:1 compression ratio, while continuing to be query-able
	Continuous archive of consolidated events to common NAS storage	Yes	Yes	Yes	Yes	Yes
	Evaluation Period – How many days for the test pilot?	30 days	30days	30 days	30 days	30 days

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

	Easy of deployment and maintenance . How many days of deployment on Master, clients?	5 days	3 – 5 days	?	3-5 days	17 days
	Technical support line availability. Technical knowledge transfer.	7/24/365	24/7/365	24/7/365	Yes	Yes
	Easy of customization	Yes Completely customized	Yes	Yes	Yes	Yes SQL, perl
	Easy backup / restore	Yes		Yes	yes	Yes Hot database backup
	Easy failover procedures	Yes, can be configured for high availability failover	Veritas or Legato Cluster and Oracle RAC	Load balancing can be applied	Multiple correlators and consoles deployable in tandem	Linux cluster Where 1/nth of total log data is stored over each on nodes with a backup of another nodes data (providing auto. sailover)
	Data compression ability - for data retention for regulatory compliance.	Yes 10:1 or 20:1	Yes 20:1 compression ratio	Yes - Adamark	Yes	Raw log data 10:1 compression ratio while query-able RDBMS compressed data is not available for querying
	Regulations and Standards for audit compliance. Audit management in place.	Who logged on when they logged , etc	Yes HIPAA, GLBA, SOX	No – only with customization	Yes	Yes

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

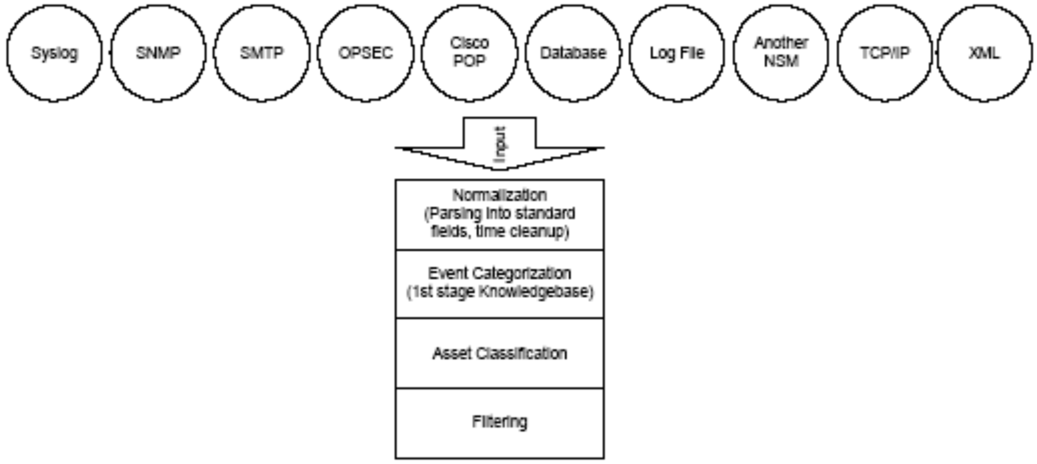
Functionality	User specific access and rights to see reports, dashboards. Limit access to administrative functionality.	Yes Access rights	Yes	Yes	Yes	Yes Role based permissions
	Highly intuitive interface to provide easy operations	Yes Realtime, dynamic, easy-to-use graphical rules system	Yes	Yes	Yes	Yes
	How plug-in updates are handled?	Yes by installation scripts	Yes	d/l via internet	On the fly integrations	Yes
SNMP	SNMP trap support?	Yes	Yes	Yes	Yes	Yes

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Functional Components for Event Logging and Correlation

[2]


Syslog
SNMP
SMTP
OPSEC
Cisco POP
Database
Log File
Another NSM
TCP/IP
XML
Input
Normalization (Parsing into standard fields, time cleanup)
Event Categorization (1st stage Knowledgebase)
Asset Classification
Filtering

Network	**Routers**	**PIX FW**	**Switches**	**SNMP**	
	syslog	syslog	syslog	syslog	
UNIX	**Mail Gateway**	**External DNS**	**Web Servers**	**Proxy Servers**	**Database servers**
	maillog	syslog	syslog	messages	syslog
Intel/Windows	**Domain Controllers PDC/BDC**	**ISS Web & MSSQL**	**Lotus Notes**	**ISA Proxy**	**VPN**
	syslog	OS Level (turn auditing ON)	OS Level (turn auditing ON)	OS Level (turn auditing ON)	syslog

WINDOWS SYSTEM:
Stores the security/system/application events in the Windows event log. Enabling the auditing feature requires planning but is necessary not to compromise the security.

SYSLOG:
Most flavors of UNIX/LINUX/Cisco/routers create their security logs through a process called syslog. It is responsible for gathering and saving all the error messages

[2] ETrust Vulnerability Manager

© SANS Institute 2005 Author retains full rights.

from the system. Syslog is a source of information on the health and security of both systems and network in general.

SNMPTRAP:
Network devices are suing SNMPtrap as an event structure. All the network devices forward events in form of SNMPtrap to a SNMP manager. Monitoring SNMP traps is essential to tracking network devices To translate them into a meaningful reports is critical for security.

Vendors charge criteria . How Vendors charge?

Products	Per events per day < 5 mln > 10 mln	Per number of devices	Number of : A.) Workstation Consoles B.) Web Browsers	Per location? A.) How many cities B.) How many offices in the same city	Per devices types ? A.) Routers - syslog B.) Switches - syslog C.) PIX FW - syslog D.) UNIX - syslog E.) Windows	Integration with Network MGMT ? e.g. (Tivoli)	Special Devices Types? A.) Security Infrastructure Devices B.) ISS IDS (Snort) Nessus
Intellitactis	yes	yes		yes	yes	yes	yes
ArcSight	yes	yes		no	yes	yes	yes
neuSECURE	yes	yes		yes	yes	yes	yes
OpenService	yes	yes		yes	yes	yes	yes
Addamark - SenSage	yes	yes		yes	yes	yes	yes
Event Tracker	yes	yes		no	yes	yes	yes

Summary of Products

Product	WWW	Master Platform	Price range	Pros	Cons
1. Intellitactis	www.intellitactics.com	Harden RH 9	120K	Great Visualization	Product stability
2. Arcsight	www.ArcSight.com	RH ES 3.0	150K	Robust reporting engine	Expensive, data management
3. neuSECURE	www.guarded.net	RH ES 3.0	60K	Web Based	Not s extensive as other products

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

4. OpenService	www.open.com	RH 9 or Windows	200K	Business centric	Not as robust as others
6. SenSage - Addamark	www.sensage.com	RH ES 3.0	?	Fast, good data management, good reports	Not quite a SIM solution yet

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005

Author retains full rights.

Conclusion

To choose and implement Event Logging and Correlation product is a challenging task because of the complexity associated with capturing, classifying, analyzing an correlating different types of information.

The product has to generate security events from the all required sources like Windows/UNIX/Network devices, database activity logs, Web servers and Mail Servers (Exchange and Lotus Notes).
The product needs to do the real time monitoring and log analysis at the same time. Most products come with the minimum tracking policy violations. Most product don't have extensive knowledge base built up and they have to be teach what needs to be capture, filter and recognize as a abnormal activity. Rules have to be written to track attacks. There are no plug ins features like Nessus has. The ability to learn from the past – the intelligence is not there yet. The trend capturing capability can be accomplished if the product works with Vulnerability Scanners or IDS products.

However all products do good job on capturing logging data across platforms in a simple accessible reporting system . All products do archive data and data mining for data discovery. Setting filters, thresholds, alarms and triggers is important and all products support it.

Again to provide continuous classification of intrusion attempts, continuous classification and follow up events and provide the ability to interpret security log data – it's not that all products provide out-of-the-box. With respect to a hundred or a hundred fifty pre-defined reports the Security Analyst's job is to automate the incident-response capability and set rules to interpret security log data.

Ideally the solution would be to have an asset management software, vulnerability scanners, intrusion detection systems and correlation software under one umbrella. To date, there is no single integrated tool that controls all steps of vulnerability and correlation management and when buying the event logging and monitoring tools we have to add for the extra price the Agents which analyze Vulnerability scanners or IDS products. The vulnerability scanners log data and host based IDS logs should be used as a data source and correlated with other events to identify when alerts correspond to a known vulnerability. The smart agents for Scanners and IDS tools need to be address to Correlation tools and can't be forgotten when delivering the Security Event Logging Correlation and Monitoring solution.

© SANS Institute 2005 Author retains full rights.

Appending A – References

1. Information Security. Departments Product Reviews. Nov. 2003
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss205_art465,00.html

2. Shipley, Greg. Network Computing. Security Information Management Tools. April 1, 2002
http://www.networkcomputing.com/1307/1307f22.html#_

3. Sidle, Scott. Information Security. Centralized Management. Jan. 2002
http://infosecuritymag.techtarget.com/2002/jan/features_command.shtml#cs

4. Insucure. Top 75 Security Tools. May. 2003
http://www.insecure.org/tools.html

5. Ubizen. From Security Monitoring to Risk Management. May. 2002
http://www.ubizen.com/c_about_us/3_investor_relations/presentations/Corporate_Customer_Case.pdf

6. NCASSR. Log Correlation for Intrusion Detection: A Proof of Concept
http://www.ncassr.org/projects/sift/papers/ACSAC03.PDF

7. Wilson, Piers. IT Security. Log analysis and correlation.
http://www.itsecurity.com/asktecs/apr4502.htm

8. PriceWaterHouseCoopers. Security Strategy & Planning. Nov. 2003.
http://www.pwc.com/Extweb/service.nsf/docid/741A32289B49E46A85256D52007A174A

9.Curry, David. Improving the security of your UNIX System. Apr. 1990
http://www.deter.com/unix/papers/improving_security_sri.pdf

10. Inellitactics
www.intellitactics.com

11. ArcSight.
www.ArcSight.com

12. Addamark
www.sensage.com

13. Guarded Net
www.guarded.net

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.