Global Information Assurance Certification Paper

SANS GSEC Practical

Kevin McIntyre
GSEC Practical Version 1.4b (1)
2/18/2003

Event Correlation Systems – The New Threat Frontline

Table of Contents

ABSTRACT 3
INTRODUCTION 3
EVENT CORRELATION 3
TYPES OF EVENT CORRELATION SYSTEMS 5
NETFORENSICS 7
GUARDEDNET NEUSECURE 9
E-SECURITY MANAGEMENT SYSTEM 12
CONCLUSION 13
REFERENCES 15

Abstract

This paper will discuss the challenge that security professionals face when trying to review the variety of logs that are produced by security devices, network devices, applications and operating systems. The paper will then provide the security professional with an alternative solution to manually reviewing the numerous log files. This alternative solution is the event correlation system. The features and functions of event correlation systems and their limitations will be reviewed as well as the different architectures and three leading products in this area of security information management.

Introduction

Companies spend countless valuable resources developing security policies and implementing security hardware and software to limit their security vulnerabilities and protect against the threats that can compromise the confidentiality, integrity and availability of their critical information assets. Government regulations such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm Leach Bliley Act (GLBA) have also required companies to ensure the protection of their data and systems. Protection of a company's information assets and reputation is why so many companies have come to realize the importance of security, and have invested so heavily in security products. The problem is that when so many security products are purchased and implemented, the amount of information that is generated can become overwhelming and extremely difficult to manage. Firewall logs, intrusion detection system event logs, operating system event logs, mail system logs, database logs, web server logs, antivirus logs, and router/switch logs all provide information that can potentially identify a threat and can contain hundreds or thousands of transactions a day. Many companies implement these products or have vendors implement the products for them only to find out later that they do not have the time, staff or knowledge to monitor the logs or to obtain any useful information from them.

Event Correlation

The time it takes to read through and analyze the vast amount of transaction logs that can be produced will make security professionals spend too much time on unimportant events and not enough time responding to significant security threats. This process is known as security information management and is the reason security event consolidation and correlation systems have become vital to the successful identification and handling of security incidents. Event consolidation brings together events from disparate systems into a central repository and event correlation monitors the various security events to determine which events are significant and relate to a particular attack.

There are a wide range of security products, network hardware, applications and operating systems available to consumers. Because of this, companies that provide event correlation systems must be prepared to provide an application that will report on the various log file formats. A vendor may be able to provide an excellent event reporting tool but if it only works with one brand of products it will be of little use in most business environments. The companies must also provide correlation applications that are not too complicated to configure and that will produce accurate results. As budgets become tight, businesses become more diligent in their expenditures, requiring companies to provide what is promised. If the vendors cannot provide the quality of product and service that is promised, the weaknesses will become widely publicized and the company's reputation will be severely affected.

Event correlation systems must be able to provide relevant information in a real-time or near real-time manner through a centralized management console. These systems must also include paging, email and remote access capabilities for contacting security administrators while they are off-site.

The longer it takes security administrators to identify the real threats and remove the vulnerabilities, the higher the risk of the threats exploiting the vulnerabilities and causing an incident. If system administrators spend too much time on false-positives (an event that is identified as an incident when it is non-existent), false-negatives (an event that is not identified as an incident when it should be) or non critical events, the real threats may pass through undetected and propagate through the network. This can cause network downtime and cost the company thousands or even millions of dollars. "In 2002, Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches." (1) According to InformationWeek, the overall cost of managing attacks and security infrastructures across the U.S. rose to about $266B. Most of this cost can be directly attributed to the labor cost involved in detecting security events and repairing the damage the breaches create. Companies cannot afford downtime that causes loss of revenue and loss of employee productivity due to security incidents but also in terms of long term damage to their reputation and customer base.

The following are some of the most serious security facts that one has to consider in dealing with security issues:

1. The SQL Slammer worm spread worldwide in 10 minutes.
2. It was estimated that malicious code cost companies around $13.2 billion dollars in 2001.(2)
3. The Code Red worm infected 359,000 servers in less than 14 hours.(2)
4. The total security incidents reported to CERT increased from 52,658 in 2001 to 82,094 in 2002.(3)

These staggering numbers show that attacks are affecting networks and systems faster than ever and are increasing in number over time. This data shows that the effects of taking too long to respond and remediate security incidents can cost companies enormous amounts of money.

Recently, while working on the SQL Slammer worm vulnerability, it became evident that it was going to be difficult to identify which systems had this vulnerability because the worm not only affects Microsoft SQL Server but Microsoft SQL Desktop Engine as well. Considering there are approximately one hundred forty eight non-Microsoft and seventeen Microsoft applications that may install SQL by default, it is not hard to see why it would be difficult to identify the vulnerable systems. In this situation a port scan had to be run against all workstations and servers to determine which systems had the vulnerability. This just goes to show how much time and money can be spent trying to identify and eliminate vulnerabilities before incidents occur.

Event Correlation systems must also be able to store and report on historical data. Historical data is necessary to identify attacks coming from the same IP address or to identify similar types of attacks that have occurred over time. This information would be invaluable when trying to prosecute an attacker that has cost your corporation millions of dollars in lost revenue due to a denial of service attack or virus infection. It would be hard to prove a particular attack when you only have a couple of months worth of data and the attack spanned over a six month period of time or longer.

Types of Event Correlation Systems

Today, there are two types of event correlation systems available. They are the rules based system and the statistical based system.

The first type is a **rules based system**. (4) In rules based event correlation and consolidation systems, patterns of known security threats are defined in a database. These patterns can be pre-defined rules provided by vendors or they can be developed by the systems administrator over time. For example, an administrator could define a rule that would monitor port scans on their network devices. If it is found that these port scans are trying to identify open telnet ports, the rule could then monitor for telnet connection attempts during a predefined period after the port scans. If a telnet connection is identified and has originated from an unknown IP address, the event correlation system would send an alert to the management console or alternatively to a pager, email address or cell phone.

This rules based type of event analysis can be compared to signature files used in virus detection software. Signatures, also know as footprints, are pieces of code that every virus contains. These virus signatures are compiled into databases that become the signature files we are familiar with and need to update on a regular basis in order to protect our systems. As you can see, a

significant weakness of this type of system is the time it takes to update the signature file and to get this file distributed to your network users. This same weakness would apply to rules based event correlation systems. If you do not update the rules on a regular basis or the rules can not be defined as fast as the viruses are created or the hackers attempt to break into your network, the system will become useless. A prime example of this issue is the recent "SQL slammer" worm. This worm infected systems globally within 10 minutes and caused denial of service problems for many large corporations, including Microsoft. If a company as large as Microsoft doesn't have the staffing or time to keep up to date with system patches, how are other companies that are not fully staffed going to be able to keep up?

The second type of event correlation system is **statistical based**. (4) These types of systems analyze events over a period of time and use weighted values to rate assets, systems and attackers. These weighted values are then analyzed to determine the risk of this type of attack occurring. These systems also set baseline levels of normal network activity and look for deviations from these normal behavior patterns that may indicate an attack. For example, a series of twenty telnet attacks may be identified on an e-commerce server that handles thousands of transactions an hour. This attack would be assigned a high rank compared to a series of ftp attempts on a web server that hosts third party informational sites. The weighted values are used to prioritize the attacks as they are identified and to filter out the more common types of events that occur on a regular basis, such as port scans with no subsequent activity on the ports being scanned.

This statistical type of analysis is performed manually by many corporations when they inventory their assets and rank them in terms of value to the company or potential loss of value if the system is attacked. Without this type of information corporations will never understand or be able to respond to incidents in an efficient and effective manner. If a company doesn't understand the value of their assets, they will definitely not understand the potential loss from their systems being hacked or infected with a virus. This type of system can also be compared to anomaly based intrusion detection systems that monitor for abnormal patterns of activity coming into a network segment and report the information to a log file.

There are an enormous number of products that claim to provide event correlation services. Some of these products include NetIQ Security Analyzer, IBM Tivoli Security Event Management, SeaGate NerveCenter, HP Openview ECS, OpenService, Inc. ThreatManager, Intellitactics Network Security Manager, Guardent Correlation Engine and ArcSight Security Event Manager. The major differences between most of these systems are the types of network devices and applications supported and the number of devices supported. I am going to review products from three well known vendors. The products I am going to

review are netForensics, GuardedNet neuSECURE, and e-Security Management System.

netForensics

The first product reviewed is from netForensics. netForensics provides a modular design with agents that support multiple devices, operating systems and applications. There are three main components that make up the netForensics security information management architecture. The three components are the database that stores the data gathered from the various log files, the correlation engine that monitors the various agents, normalizes and correlates the data for the database, and the agents that can process data from multiple security devices simultaneously. The scalability of this product can be enhanced by installing multiple engines to process the data and send it to one or multiple databases. If multiple databases are used, a master database must be configured to consolidate and correlate the data from the various distributed databases.

Figure 1 below is a netForensics diagram that illustrates the architecture of the system. (5)

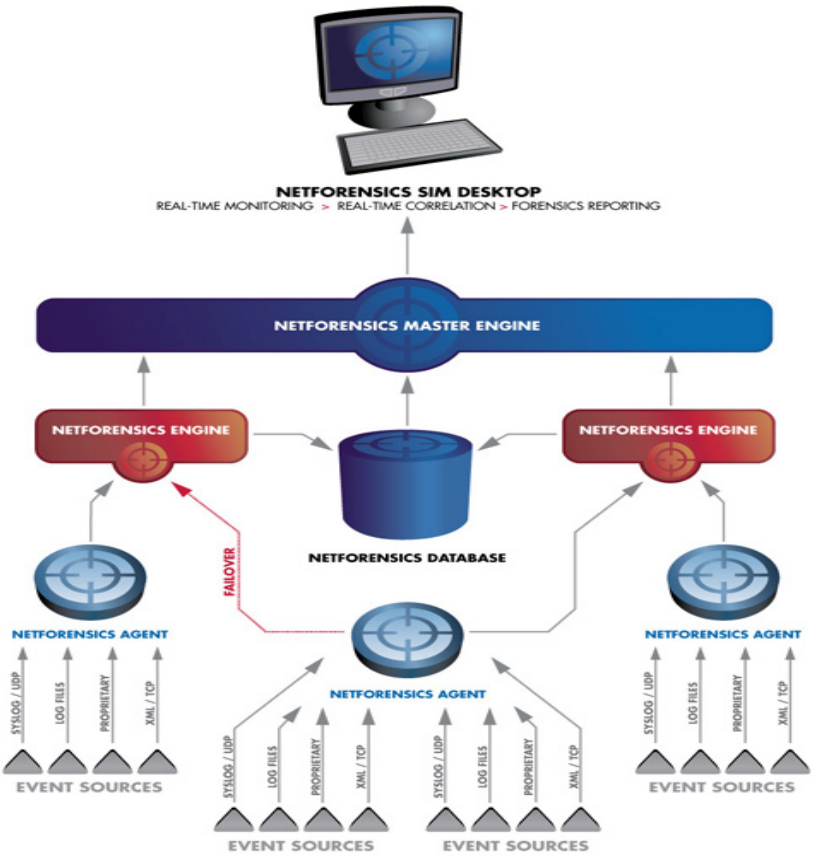


Figure 1

netForensics will run on Solaris 2.6, 7, and 8 and higher or Linux 6.1 and above. Its hardware requirements are not very restrictive either. It will run on an Intel system with at least a Pentium III 500 MHz processor, 768 MB RAM and 12 GB of free disk space.

The netForensics agents report data to the engine in Java and XML format using the TCP protocol and from the engine the data can be sent to several different sources. Users can also customize the Universal Agent to support other products. The netForensics correlation engine is the heart and sole of the application and controls the normalization of data as well as the scheduling of reports for distribution. Once the data is processed by the engine and stored in the database, the data can be sent to the console/client in HTML format via the HTTP protocol or through SNMP traps sent via the SMTP protocol to an external device such as an email client or pager.

The following is a list of the products supported by the netForensics security information management system: (6)

Anti-Virus	**Web Servers**	**Databases**	**VPNs**
Norton Anti-Virus (Symantec)	Apache (Apache)	Oracle	Cisco VPN 3000 Concentrator
InoculateIT (Computer Associates)	Netscape Enterprise	Sybase	Check Point VPN-1
Virus Scan (McAfee/NAI)	IIS (Microsoft)	Informix	
		SQL Server	
		MySQL (MySQL AB)	

Operating Systems	**Enterprise Management Policy Monitoring and Configuration**	**Host Integrity**
Solaris	SolSoft	Cisco Router ACLs
Linux (Various)	CiscoWorks	
Windows NT	Websense	
Windows 2000	Optivity	
SunOS	Unicenter	
HP-UX	HPOpenview	
IRIX (Silicon Graphics)	Micromuse	
AIX (IBM)	Tivoli	
Open BSD	Axent ESM (Axent/Symantec)	
SuSE		

netForensics provides a variety of reports for management and systems administrators to use for monitoring daily security operations. Some of the reports include: top ten intruders, registry access summary, authorization and access summary and telnet connection summary. This is only a partial list of the reports provided. A more comprehensive list of reports can be obtained on the netForensics website.

NetForensics recently joined forces with HYPERNOC, Inc. which will allow them to include other sources of information in their information management solution. (7) Some of these sources of information include: help desk activity, network configurations, and asset attributes. This data will increase the product's capability to provide more comprehensive information on the impact of a security threat to a corporation's business operations.

netForensics received Network Computing Editor's Choice Award in April of 2002 and their Well Connected Award for the best security information management solution in May of 2002. (8) The product has also been nominated for Information Security Magazine's Information Security Excellence Award and is listed on their website as an information security hot pick for January 2003. (9)

GuardedNet neuSECURE

The next product reviewed is GaurdedNet neuSECURE. GaurdedNet refers to the different types of correlation as micro/atomic level correlation and macro/fusion correlation. The micro correlation system is similar to the rules based system that I discussed above with additional searches and the macro correlation system is related to the statistical system. They also refer to security information management as security event management. GaurdedNet provides a clear definition of correlation that is helpful in understanding the security event management process. They define correlation as "taking many isolated security events and putting them together to create one single relevant security incident" which they also refer to as the security event chain. (10) This definition breaks down event correlation into a simplistic view that is understandable to security experts as well as management, network administrators and the various support staff.

GuardedNet breaks the micro and macro event correlation systems into many different correlation types. (11) The micro correlation types include:

1. Field Correlation – performs a basic search on security devices for certain criteria such as the telnet traffic on port 23.
2. Auto Correlation – all fields are compared to determine if there is a correlation between them.
3. Rule Correlation – defined rules are used to determine if events are correlated.
4. Packet Correlation – payloads of packets are monitored for correlations.

The macro correlation types are:

1. Profile Correlation – remote port scans and finger information provide information that can be examined to identify attacker patterns.
2. Vulnerability Correlation – mapping IDS events against vulnerabilities on a particular host. Requires a vulnerability scanner.
3. Open Port Correlation – determining the probability of attack by examining open ports on a system.
4. Route Correlation – determining the route an attack took to potentially use to block the source.
5. Role Based Correlation – analyzing computer and user behavior and detecting anomalies in this behavior.

6. Bayesian Correlation – anticipates what an attacker will do based on statistics and probability of two variables.
7. Neural Correlation - Similar to Bayesian but can use more than two variables.

These types of micro and macro correlation types are mainly advanced versions of the rules base and statistical systems discussed earlier.

Figure 2 is a diagram from GuardedNet that illustrates the architecture of the neuSECURE system. (12)

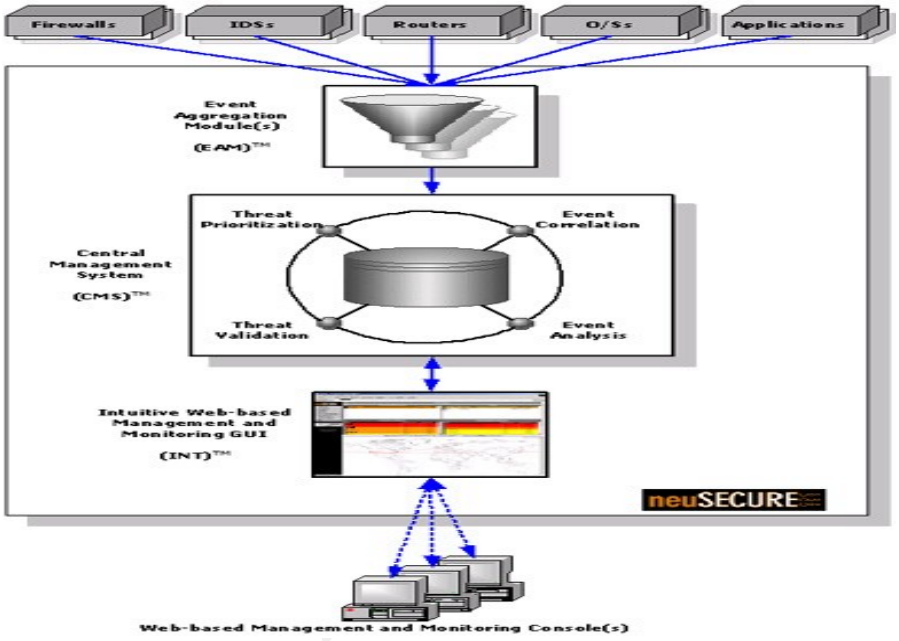


Figure 2

GuardedNet did not provide any information about the hardware or software requirements of their product on their web site or in any of their product literature.

GuardedNet neuSECURE's architecture is modular in design but is different from many of the other products in that an agent does not need to run on the device that is being monitored. The benefit to not having an agent run on each of the systems is that it helps reduce the load on the systems and it helps reduce the troubleshooting steps necessary when problems occur. It also reduces the scope of the deployment process by not having to touch each of the devices or systems in some way. neuSECURE ships with built-in support for a wide variety security devices and applications but an add-on agent is available for devices not supported by default. The next component in neuSECURE's architecture is the Event Aggregation Modules that collect the data and normalize it into a common format. The final component of this system is the Central Management System. This part of the architecture is where the correlation engine and the database exist. GuardedNet neuSECURE also provides a web-based interface that is

helpful for monitoring and managing incidents throughout the identification and remediation process.

Gaurdednet neuSECURE's reporting capabilities are provided by its Analytics and Reporting module. The reporting module allows scheduling reports on an hourly, daily, weekly, monthly or ad-hoc basis. GaurdedNet claims that a variety of pre-configured reports are available for event analysis, threat analysis, and administration but the problem is that they do not define what types of detailed reports are available. The data from the events can be displayed in a chart/graph view or via detailed lists. The product also provides a customizable report writer that enables security administrators to define their own reports.

An additional feature of the neuSECURE product is its Host Investigative Toolkit that is a group of third-party tools to help in forensic analysis when an incident does occur. (13) The HIT includes tools for doing remote host lookups, operating system queries, port scans, and traceroutes. GuardedNet claims to have reduced the average time spent investigating and responding to an attack from 30 minutes to less than 3 minutes using the neuSECURE product.

GuardedNet neuSECURE was a finalist for Network Computing's Well Connected Award for the best security information management solution in May 2002. (14) The product is also listed on Information Security Magazine's website as an information security hot pick for January 2003. (15)

The following is a list of the products supported by neuSECURE: (16)

Antivirus
McAfee (Network Associates)
Norton (Symantec)

Operating Systems Logs
Unix Syslog
Linux Syslog
Microsoft NT/2000/XP

Routers/Switches
Cisco router series
Cisco Catalyst/Switch series
VPN:
Check Point VPN-1 v 4.1
Nortel Contivity

Firewalls:
Check Point Firewall-1 v 4.x
Cisco PIX (all supported versions)
IP Chains/Tables
Netscreen v 3.x
StoneSoft's StoneGate 2.x
Secure Computing's Sidewinder
Secure Computing's Gauntlet
Symantec's Enterprise Firewall/Raptor v 7
OpenBSD Firewall (IPF/PF)
Sanctum AppShield (Application Firewall)

Intrusion Detection (Network Based)
ISS RealSecure (all supported versions)
SNORT (all supported versions)
Enterasys Dragon
Cisco Secure IDS v 3.x
ISS BlackICE Sentry
Lancope StealthWatch
Intrusion's SecureNetPro v 4, 2000, 5000
NFR NID 100 and 200
ForeScout
Top Layer Attack Mitigator
Symantec NetProwler
Network Ice

Intrusion Detection (Host Based)
Tripwire (all supported versions)
Symantec Intruder Alert (ITA)
ISS OS Sensor
ISS Server Sensor (all supported versions)
Enterasys Dragon Squire
Entercept v 2.x
Okena StormWatch

Vulnerability Assessment	VPN
Nessus	Check Point VPN-1 v 4.1
NMAP	Nortel Contivity

e-Security Management System

The final product reviewed is e-Security Management System's real time control center. e-Security provides a modular approach to security information management similar to netForensics, and GuardedNet neuSECURE's systems. The e-Security architecture is designed a little different than the other products. It is a combination of three e-Security products: e-Wizard, e-Sentinal, and e-Security Advisor. The architecture is divided into three levels. The first level defines the event sources of the infrastructure. The second level includes data gathering and communication and consists of the agents and e-Wizard and the third level is the heart of the system that provides the correlation and reporting functions and consists of the e-Sentinal. The e-Security Advisor provides incident response functions and includes a cross-reference between the e-Security real-time alert data and the Symantec SecurityFocus Vulnerability Database.

Figure 3 is an e-Security diagram that illustrates the architecture of the e-Security Management System. (17)

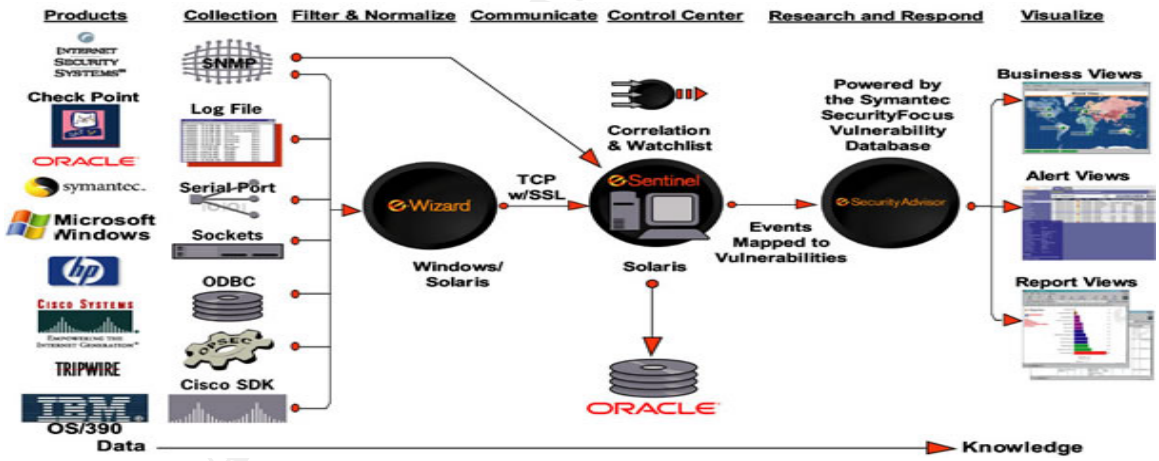
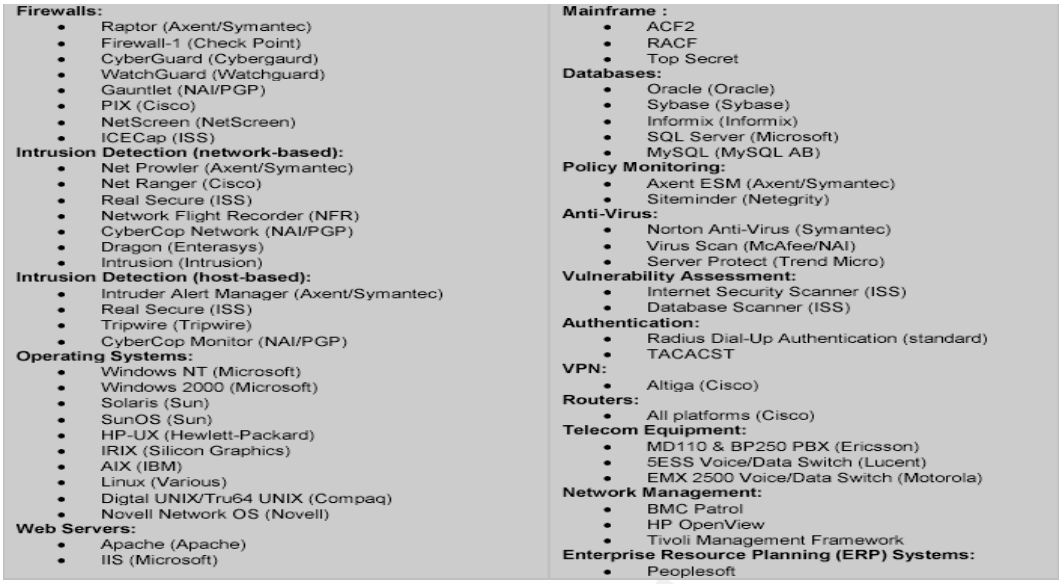


Figure 3

The e-Security Management System will run on a Sun UltraSparc server with a minimum of one 400 MHz processor running Sun Solaris 2.6 or higher, 256MB of RAM and 4 GB of free hard drive space. It will run on an Intel processor of 300 MHz running Windows NT 4.0 or Windows 2000 with 128 MB of RAM and 12 GB of free hard drive space.

The following is a list of the products supported by the e-Security Management System: (18)



Firewalls:
- Raptor (Axent/Symantec)
- Firewall-1 (Check Point)
- CyberGuard (Cybergaurd)
- WatchGuard (Watchguard)
- Gauntlet (NAI/PGP)
- PIX (Cisco)
- NetScreen (NetScreen)
- ICECap (ISS)

Intrusion Detection (network-based):
- Net Prowler (Axent/Symantec)
- Net Ranger (Cisco)
- Real Secure (ISS)
- Network Flight Recorder (NFR)
- CyberCop Network (NAI/PGP)
- Dragon (Enterasys)
- Intrusion (Intrusion)

Intrusion Detection (host-based):
- Intruder Alert Manager (Axent/Symantec)
- Real Secure (ISS)
- Tripwire (Tripwire)
- CyberCop Monitor (NAI/PGP)

Operating Systems:
- Windows NT (Microsoft)
- Windows 2000 (Microsoft)
- Solaris (Sun)
- SunOS (Sun)
- HP-UX (Hewlett-Packard)
- IRIX (Silicon Graphics)
- AIX (IBM)
- Linux (Various)
- Digtal UNIX/Tru64 UNIX (Compaq)
- Novell Network OS (Novell)

Web Servers:
- Apache (Apache)
- IIS (Microsoft)

Mainframe :
- ACF2
- RACF
- Top Secret

Databases:
- Oracle (Oracle)
- Sybase (Sybase)
- Informix (Informix)
- SQL Server (Microsoft)
- MySQL (MySQL AB)

Policy Monitoring:
- Axent ESM (Axent/Symantec)
- Siteminder (Netegrity)

Anti-Virus:
- Norton Anti-Virus (Symantec)
- Virus Scan (McAfee/NAI)
- Server Protect (Trend Micro)

Vulnerability Assessment:
- Internet Security Scanner (ISS)
- Database Scanner (ISS)

Authentication:
- Radius Dial-Up Authentication (standard)
- TACACST

VPN:
- Altiga (Cisco)

Routers:
- All platforms (Cisco)

Telecom Equipment:
- MD110 & BP250 PBX (Ericsson)
- 5ESS Voice/Data Switch (Lucent)
- EMX 2500 Voice/Data Switch (Motorola)

Network Management:
- BMC Patrol
- HP OpenView
- Tivoli Management Framework

Enterprise Resource Planning (ERP) Systems:
- Peoplesoft

In 1999, e-Security was the first company to come out with a security information management product (19) and has been given a 5 star rating by SC Magazine. (20)

Conclusion

Event correlation will continue to become a critical piece of the information security infrastructure of corporations as the complexity and number of security devices increases. As you can see from the information provided, companies have many different avenues to pursue when it comes to event correlation systems. The difficult part of the process is filtering through all of the different products, determining which one will best fit the needs of your particular environment.

Another factor that will play a major role in the decision making process is the cost of the products being reviewed. The goal of security information management systems is to reduce the total cost of ownership of security devices by reducing the time security professionals spend on threat analysis and incident management, but when these products can cost anywhere from $45,000 to $100,000 and even up to $300,000 or more depending on the number of devices supported, it may be hard for smaller companies to justify their purchase.

The initial cost alone may eliminate these products from being purchased by many smaller companies but cost alone should not be the only factor considered when doing your research. A cost-benefit analysis or return on investment analysis should always be completed when making major infrastructure decisions. You may find that the benefits from protecting your data far outweigh

the cost of implementing the solution. It is often hard to put a price on the loss from competitors obtaining your confidential company data or from not being able to conduct business due to network outages. Is your company worth $45,000, $100,000 or more? This is the real question! Network attacks can lead to the long term failure of your company!

All of these systems provide real–time threat analysis as well as support for a wide range of security products, applications, and operating systems. They also have web reporting capabilities, historical data storage, and remote management solutions. The main difference between these systems is the number and types of devices supported, correlation techniques used and the types of reporting provided. GuardedNet and e-Security could both have done a better job of defining the default reports that are available while netForensics did well in this area. netForensics and e-Security both provided support for a wider variety of products than GuardedNet neuSECURE but neuSECURE added a nice feature with its incident response and forensics solution. netForensics came out on top in Network Computing's Editor's Choice Awards because of its reporting capabilities and it had the fewest reported problems. (14) It will be up to you to decide which solution best fits your infrastructure needs based on the information provided in this paper. This paper should provide you a firm starting point of what to look for in a security information management solution.

References

General References

1. Computer Crime and Security Survey
   Computer Security Institute, April 2002
   http://www.gocsi.com/press/20020407.html

2. Security Stats.Com, Inc., 2002
   http://www.securitystats.com/sspend.asp

3. Carnegie Mellon University, January 21, 2003
   http://www.cert.org/stats/cert_stats.html

4. Comprehensive Correlation - A Two Tiered Approach, netForensics, Inc.
   http://www.netforensics.com/whitepapers.html

5. netForensics, Inc., 2003
   http://www.netforensics.com/nf/documents/pr_architecture.asp

6. netForensics, Inc., 2003
   http://www.netforensics.com/nf/documents/pr_devices.asp

Web Sites

netForensics, Inc. – www.netforensics.com

7. PRNewswire, October 22, 2002
   http://industry.java.sun.com/javanews/stories/story2/0,1072,48720,00.html

8. CMP Media, LLC, May 7, 2003
   http://www.netforensics.com/editors.htm

9. Information Security, a division of TruSecure Corporation, January 2003
   http://www.infosecuritymag.com/2003/jan/products.shtml

GuardedNet, Inc. – www.guarded.net

10. GuardedNet, Inc, 2003
    http://www.guarded.net

11. **Event Correlation – Security's Holy Grail? –** A GuardedNet Whitepaper, GuardedNet, Inc., June 2002
    http://www.guarded.net/literature.html

12. GuardedNet, Inc, 2003
    http://www.guarded.net/arch.html

13. GuardedNet, Inc, 2003
http://www.guarded.net/iwf.html

14. CMP Media LLC, 2002
http://www.nwcwellconnected.com/newfinal.asp

15. Information Security, a division of TruSecure Corporation, January 2003
http://www.infosecuritymag.com/2003/jan/products.shtml

16. GuardedNet, Inc, 2003
http://www.guarded.net/supp.html

e-Security, Inc - www.esecurityinc.com

17. e-Security, Inc, 2003
http://www.esecurityinc.com/products/architecture.asp

18. e-Security, Inc, 2003
http://www.esecurityinc.com/products/agents.asp

19. e-Security, Inc, Greg Stock, November 11, 2002
http://www.esecurityinc.com/news/releases/advisor.htm

20. West Coast Publishing, 2001
http://www.scmagazine.com/scmagazine/sc-online/2001/review/055/product.html

Additional Information

http://www.networkcomputing.com/1307/1307f2.html
http://www.esecurityplanet.com/views/article.php/10752_1501001
http://www.cisilion.com/dashboard.htm
http://www.cert.org/stats/cert_stats.html
http://www.securitystats.com/news.asp
http://www.esecurityinc.com/ProductCorporateLiterature/eSentinel.pdf
http://www.gocsi.com/press/20020407.html
http://wwwmnmteam.informatik.uni-muenchen.de/projects/evcorr/

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event