Global Information Assurance Certification Paper

netForensics® – A Security Information Management Solution
Michael B. Godfrey
Version 1.2f

Introduction

netForensics is a security information management (SIM) solution that positions itself as a central point for your security information that is collected by various devices. This scalable solution increases the manageability of multiple security countermeasures, thus increasing your overall security posture. It allows customization of alerts and reports, to better manage the flow of security information within an organization. netForensics eases the burden of auditing policy compliance, by providing a common framework for disparate alerting and reporting facilities.

Why you Need a Security Information Management Tool

Say you manage a large enterprise and are responsible for security. You have firewalls protecting your perimeter and you have an Intrusion Detection System (IDS) deployed across your network segments. You also use some type of enterprise management platform software to monitor availability. If you think your work is done here, I venture to say you have an incorrect perception of your security posture, or are spending quite a bit more money managing security than you should. What you need is a SIM solution. This is software that pulls these things together and should complement your enterprise management platform.

With the proliferation of security products today there is a need for SIMs that can provide a common framework for managing security. Single vendor solutions across an enterprise are a thing of the past. One stop shopping rarely fulfills all the requirements when it comes to meeting information systems needs. Technologies come more and more from niche players; this is especially true in the security arena.

Product Overview

Single server netForensics deployment operating systems and hardware requirements:

Operating Systems

- Solaris 2.6/7/8
- Red Hat Linux 6.1 and 6.2
- Windows NT 4.0 Service Pack 6/6a
- Windows 2000 Service Pack 1

Hardware Platforms

Intel Platform:

- Intel Pentium III 500 MHz

- 768 MB RAM
- 12 GB free disk space

Sparc Platform:

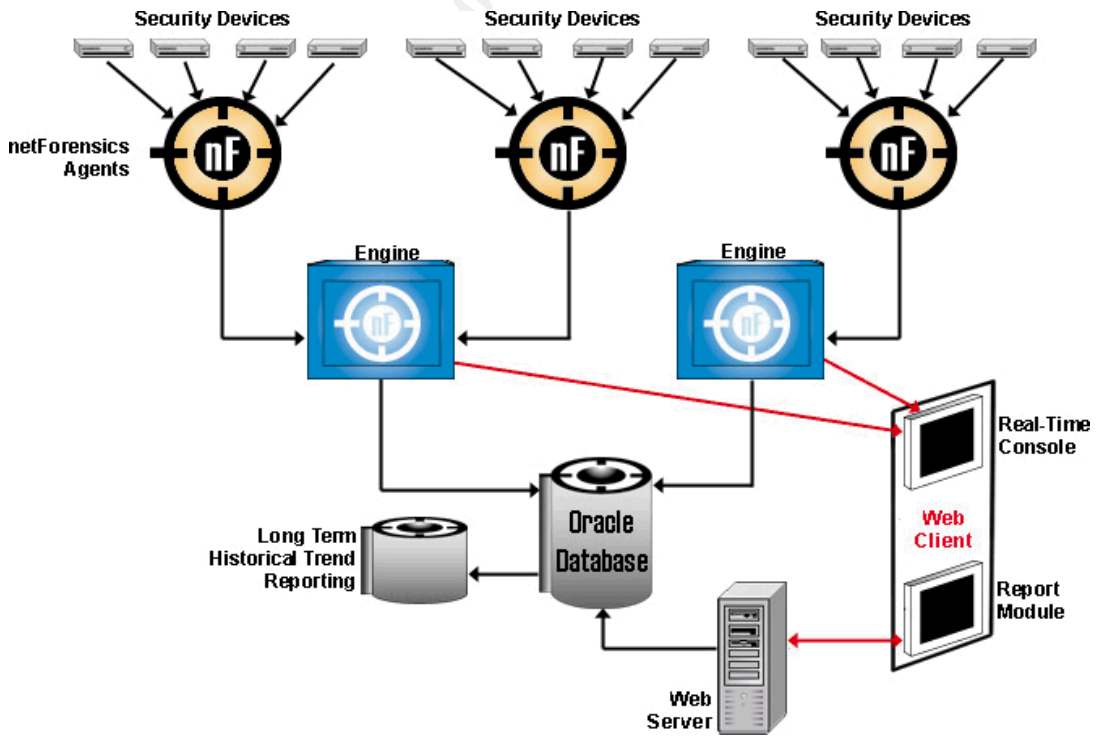
- Ultra Sparc-IIi 333 MHz
- 768 MB RAM
- 12 GB free disk space

netForensics has three main software components that drive its core functionality:

- nf Agents/Universal Agent
- nf Engine
- Oracle database

The nf Agents collect messages and alerts from their manageable devices. Out-of-the-box, netForensics has support for most major vendors. However, with their Universal Agent, you can easily develop support for additional devices using a standard XML based language. These agents are interfaces to disparate security devices and applications that normalize the data, giving each event/message a netForensics event ID. This allows the nf Engine to do analysis and meaningful correlation, then to alert when necessary. All this data is housed in an Oracle database. The database feeds both the ad hoc reports as well as the scheduled reports that you can setup through the web based front end.

Figure 1[1]



netForensics – The Security Information Management Tool

netForensics does well in the five areas one should consider when looking at SIMs:

- Scalability
- Security Analysis and Forensics
- Notification Management
- Reporting
- Enterprise Management Compatibility

Scalability

In large enterprise networks, things can get very complex. Some networks start small or medium sized, then grow into large complicated ones very quickly. Others take decades in reaching their large size. These can be some of the most difficult networks to implement brand new security measures into. There tends to be different requirements for individual segments of the larger network. Also, there are many different technologies in the installed base to meet those segments disparate needs. One thing almost all the measures have in common is the enormous amounts of data that they generate. netForensics addresses these challenges with their use of Component Architecture.

These components can be run on one box, or on separate boxes if you purchase a distributed license. The ability to separate the components and tune the boxes to their respective tasks, allows for significant scalability. As the organization grows so too will the need for additional security devices. netForensics, in a distributed deployment, can handle additional devices by putting more agent boxes in front of the nf Engine server. Using the SyslogFile Agent, netForensics can process over 8,000 events per second.[2] The nf Engine also does aggregation of messages from devices. This results in better data management in the database.

In a distributed environment, there is always a need for secure communications between devices. netForensics has the ability to communicate securely, between devices, with some configuration.

> "The communication between nF Agents and the nF Engine is XML over TCP, which uses nfetp (netForensics event Transfer protocol). The communication between the nF Engine and the nF Database is pure JDBC. These communications can be secured using third party JDBC drivers or by enabling IPSEC on the host level and building a secure Tunnel."[3]

This is a growth area for netForensics. They will have SSL out-of-the-box in Version 3.0 of their product, for the Web Server piece. This was something glaringly missing in

Version 2.3 of the product. The Web Server allows you to do administration and run reports from a web browser, Netscape or Internet Explorer. While customization of the Web Server, Apache or Internet Information Server, to use SSL was possible, it was more difficult than necessary. With secure communications in place, netForensics, and any IS System for that matter, can more easily be placed across your network, with reduced risks of sensitive security conversations being compromised.

Security Analysis and Forensics

Complete Security Picture

The main goal is to get as complete and accurate a picture, as possible, of your organization's security posture. This picture is developed from correlating all your countermeasures in a consistent way and marrying that with historical analysis and forensics.

Correlation and Analysis

Cross device correlation is only possible after you establish a common framework between the systems.

> "Information from firewalls, Intrusion Detection Systems, VPNs, applications and host-integrity systems is intelligently analyzed. Rule-based correlation techniques provide the logic required to identify various patterns of threats. The netForensics rule-set…can be modified by the administrator to suit each client's particular requirements."[4]

One cannot stress the importance of apples to apples comparisons of security information. This correlation work done by netForensics, can save you many man-hours of pouring over non-actionable data. However, there is some upfront investment a corporation must make. Organizations need to spend time gaining an understanding of what the scoring mechanisms are that they put in place, lest they get an inaccurate picture from what information is presented to them.

Historical Analysis

All messages delivered to netForensics are housed in an Oracle database. If you have the disk space, I suggest keeping the information as long as possible for later review. This information is invaluable for forensics. In addition, you can do historical comparisons if you retain a large enough data set.

Notification Management

To truly increase your security posture, you need to monitor, not only your traffic, but the alerts generated by your various security countermeasures. However, making sense of all the information being gathered can be a Herculean effort. According to Bruce Schneier, "The future of digital systems is complexity, and complexity is the worst enemy of

security."[5] We see just this issue in the security arena with different vendor's solutions, all having their own way of scoring the severity of incidents and the alerting and reporting of these events. So how does one reduce the complexity inherent in managing multiple security systems? The answer lies in the normalization of disparate alerting facilities, such as ISS RealSecure® and Cisco PIX IDS®, and implementing a common severity rating system. Once you bring together security alerts under a common umbrella, you can begin to bring sanity to your monitoring and alerting efforts. netForensics has native agent support for the following devices, which allows it to receive and normalize alerts from:

Figure 2[6]

Intrusion Detection (network-based)
Net Ranger (Cisco)
Cisco IOS IDS
Dragon Sensor
Snort
Real Secure (ISS)

Intrusion Detection (host-based)
Entercept
RealSecure (ISS)
Dragon Squire

Operating Systems
Solaris (Sun)
Linux (Various)
Windows NT (Microsoft)
Windows 2000 (Microsoft)

Firewalls
PIX (Cisco)
Cisco IOS Firewall
Firewall-1 (Check Point)

VPNs
Check Point VPN-1
Cisco VPN 3000 Concentrator

Alerting

Event Analyzer

netForensics' Event Analyzer allows network managers to immediately sift through large volumes of data, focus on high-risk security breaches and track them. It analyzes, reports and correlates all security violations across various network devices and applications.[7] The nf Engine drives this correlation process. It also then delivers notifications based upon criteria that you select.

Through the web based administration tool, you can select what severity level messages you want to deliver to either the Real-time Alarm Console, or to the database for ad hoc and scheduled reporting. You have the ability to select only the most critical events for real-time alerting, while still capturing the totality of messages for historical and archival purposes. You can also cull specific message types from going anywhere, if they are just "noise" on your network. Since one network's security incident is another network's false positive, this ability to tune data collection and subsequently backend alerting, is a stellar feature.

Real-time Console

netForensics' Alarm Console provides a real-time status of monitored devices with a detailed, scrolling Alarm Viewer accessible from any Java-enabled browser.[8]
Having a single console monitoring several security products helps an organization in many ways. First, it reduces costs associated with training operators on multiple technologies. Second, you get a more complete security picture from the normalized data being alerted via a common severity scheme. Finally, the operational benefits of changing alerts and reporting from a single technology, eases administration. This should not be overlooked as a value point. This provides, operational teams, the incentive to remain vigilant through change management and ever changing security requirements. Without this flexibility, an organization might otherwise choose to avoid the, sometimes significant, overhead of tuning and refining their alerting and reporting strategies.

Useful Reporting

Reports need to provide useful information. Just having pretty reports does not meet the goal of increased security tracking. netForensics reports leave a little to be desired, from the visually pleasing standpoint. However, they make up for it in their usefulness to security engineers. The ad hoc reports allow you to query the data in many different ways. This allows you to not only find the information that is important to your organization, but also lets you have the data presented to you in a way that makes the "bigger picture" more evident, in regards to anomalous traffic.

You can find the breakdown of report categories and their intended audience here.[9] As mentioned before, the less-than-pretty presentation of information makes these reports less likely a candidate for upper management. They have put a lot of effort into delivering the important detail to you in their reports. This is a great thing for the operations people, the ones really looking at the reports anyway. The web interface does a great job of letting you run ad hoc queries and scheduling regularly run reports, which are really the same canned queries minus the ones that require input.

All reports give you information back in three ways: 1) Columnar output 2) Bar Graph 3) Pie Chart. The columnar data is where you will spend the Lion's Share of your time. The Bar Graphs and Pie Charts tend to leave you wanting. The information is rarely presented in a useful way in these two outputs. The data lends itself to be better represented in a histogram like MRTG[10] output. netForensics is aware of the need for improved graphing and aesthetics in their reports. Jim Stemme, Eastern Regional Manager for netForensics, has stated, "this as a major goal in future releases."[11]

One thing that can be done in netForensics to help increase both the usefulness and the aesthetics of reporting is customizing what information you want to report on. The significant amount of information collected by default, all shows on the reports, regardless of its usefulness. This "pollution" of the database also detracts from the beauty of the reports. The nf Engine gives you the ability to block any messages you want from entering the database, and subsequently appearing on the reports. There is no need to

visit the individual reporting devices to implement this policy change, one centralized change to the nf Engine has the immediate effect across the board.

Enterprise Management Compatibility

Large enterprise environments have a different set of requirements when it comes to security technologies. They need more than just a robust incident alerting technology. They need something that will achieve their business goals as well as meet their technical needs of identifying malicious behavior. If an enterprise cannot manage their security technologies and processes effectively, it does not matter what other technologies you put in place to identify threats. Today's networks have grown immeasurably more complex and difficult to manage. Computer Associate's TNG Unicenter®[12], or IBM's Tivoli®[13] products are necessary, to effectively monitor and manage all the devices that live on a large enterprise network.

Security, like network management, needs an enterprise class framework to bring together the multitude of security countermeasures that larger networks may employ. Ideally, security is on par with availability in your network architecture. However, as is many times the case, security rides shotgun to availability, so there is a need to have your security management software complement your enterprise management software. Netforensics fills this niche very well.

netForensics can generate SNMP Traps, which is a standard function these days. This allows for seamless integration into various other systems, by using this common transport scheme. When an event happens, netForensics can complement an organization's architecture by letting the infrastructure people know something is going on right away. These organizations are typically the first to implement 24x7 coverage. This way previous investments in availability can be leveraged and future costs for training can be minimized. After hours operators can watch and manage consoles from enterprise availability products and yet still be aware of security events.

Conclusions

Increasing your security posture today requires the ability to handle and analyze larger amounts of data than ever before. Complex networks need SIMs to monitor and manage output from disparate security countermeasures. netForensics is a SIM solution that can make this job more achievable. By providing a common framework for alerting and reporting, netForensics helps organizations better monitor and manage their security information. Armed with this data, organizations will be more able to track adherence to the security policy, and subsequently take the necessary steps to see that it is enforced.

References

[1] "A Distributed Architecture Delivering Scalability and Performance." netForensics®

Online Documentation. URL: http://www.netforensics.com/architecture.html (29 November, 2001)..

[2] "Question #10." Online Technical FAQ. URL: http://www.netforensics.com/techfaqs.html (29 November, 2001).

[3] "Question #5." Online Technical FAQ. URL: http://www.netforensics.com/techfaqs.html (29 November, 2001).

[4] "Universal Correlation." Product Analysis. URL: http://www.netforensics.com/analysis.html (5 December, 2001).

[5] Schneier, Bruce. "Software Complexity and Security." Crypto-Gram Newsletter. March 15, 2000. URL: http://www.counterpane.com/crypto-gram-0003.html - SoftwareComplexityandSecurity (4 December, 2001).

[6] "Question #8." Product FAQ. URL: http://www.netforensics.com/pfaqs.html (17 January, 2002).

[7] "Event Analyzer." Software Solutions to Secure the Enterprise. URL: http://www.netforensics.com/products.html - three (18 January, 2002).

[8] "Real-Time Alarm Console." Software Solutions to Secure the Enterprise. URL: http://www.netforensics.com/products.html - three (18 January, 2002).

[9] Product Reporting. URL: http://www.netforensics.com/reporting.html (18 January, 2002).

[10] "MRTG Index Page." What is the Multi Router Traffic Grapher? URL: http://www.stat.ee.ethz.ch/mrtg/ (18 January, 2002).

[11] Stemme, Jim. Personal Interview. (4 January, 2002.)

[12] "Configuration Management and Operations." URL: http://www.tivoli.com/products/solutions/operations/news.html (28 December, 2002).

[13] "Unicenter Network and Systems Management 3.0." Enterprise Management. URL: http://www3.ca.com/solutions/product.asp?id=2869 (28 December, 2002).

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS