Global Information Assurance Certification Paper

Increasing Security Effectiveness with netForensics

Matthew P. Steiniger
GSEC Practical v1.4b, Option 1
December 18, 2003

Matthew P. Steiniger
GSEC Practical v1.4b, Option 1
December 18, 2003

Increasing Security Effectiveness with netForensics

Abstract
The purpose of this paper is to explain netForensics software, and to explain the impact that netForensics software can have on an organization's security effectiveness.

The amount of data collected by firewalls and event logs is increasing every day. In order to cope with this increasing amount of data, businesses will need new technologies to manage the data collected by firewalls and event logs. That is where netForensics comes in. NetForensics is a Security Information Management (SIM) solution designed to handle the data output from many of the security products and devices currently being used by today's businesses.

This paper is intended to help familiarize the reader with netForensics software. This paper will cover; the benefits of netForensics, explain how a SIM works, explain how netForensics works, highlight the capabilities of netForensics, why netForensics software is a good idea, and even some real world experiences gained from using this software firsthand.

The Problems

Security is not cheap. Fortune 1000 companies spend an average of five to ten million dollars a year on security threat costs. Every year the cost of information technology security related products increases (netForensics, "Security Information Management"). This increase is not just caused by increasing prices. New technologies and new vulnerabilities emerge every day. Along with these new technologies and vulnerabilities come new costs for securing them.

Keeping track of network intrusions and attempted exploits can generate a lot of data. In a typical enterprise one device can create up to one gigabyte of alert information on it's own. One IDS sensor can produce up to 500,000 messages a day (netForensics, "Security Information Management"). Now imagine how many security devices your organization has. Security personnel are constantly monitoring firewalls, intrusion detection devices, and system logs. New data arrives considerably faster than even the most prepared security team can effectively handle.

Managing large amounts of data and making a forensic analysis is incredibly time consuming. During the time spent analyzing redundant data productivity is lost, and many network intrusions could have occurred (netForensics, "Security Information Management"). Minimizing the amount of redundant data that is

reviewed by security personnel can save time. These savings in time add up and result in increased productivity.

The Solution

The solution to these problems is a Security Information Management (SIM) solution. A SIM allows real-time analysis of various types of security related data (netForensics, "Security Information Management"). During data collection, a SIM organizes and removes redundant data. A SIM also provides a single access point for all of the security data collected from the many security devices today's businesses need (netForensics, "Security Information Management").

So How Does a SIM Work?

The work a SIM performs is normally divided into four phases. The first phase is normalization. Normalization involves collecting data from security devices and putting it into a context that is easier to understand. Normalization is not an easy task because often in the security world there are no set standards for collecting or naming data. Many times the same exploit may be referred to by different names from vendor to vendor (netForensics, "Security Information Management"). Even antivirus companies do not always provide the same name for viruses that are found. To collect data NetForensics utilizes more than 30 device-specific agents that can be placed on systems to collect data in a normalized fashion. For those devices that netForensics does not currently have specific agents for there are universal agents. Universal agents are just as effective as device specific agents, however they require an additional level of setup and preparation (netForensics, "Real-Time Correlation").

The second phase is aggregation. Aggregation is the removal of redundant or duplicate event data. During this phase netForensics begins by ordering the collected data into distinct categories (netForensics, "Security Information Management"). NetForensics places events in separate event categories that allow the same attack to be identified similarly from multiple devices even though the devices may not use the same name for that attack. Another event that occurs during aggregation is "system scoring", which is a term that describes the application of a numeric system to different data that is received. System scoring is used to provide a way to rank threats according to their significance (netForensics, "Security Information Management").

The third phase is correlation. Correlation is the process of analyzing aggregated data to determine if there is a pattern. These patterns are then compared to specific attack signatures to determine whether or not there was an attempted Denial of Service (DOS), or some other type of attack (netForensics, "Security Information Management"). NetForensics uses advanced correlation techniques that go beyond normal attack detection. NetForensics allows for an "if", "then", "else" logic to be used in attack detection. NetForensics uses the example that: if we receive a reconnaissance attempt from the firewall against the DNS server, then if we receive one or more exploit attempts against the DNS

server, then send a notification to the operator. These “if/then” correlations can be used to identify different patterns as higher threat levels. The advantages of these advanced correlation techniques include a reduction in the number of false positives, and identification of security incidents (netForensics, “Correlation”).

The final SIM phase is visualization. This is the graphical representation of the security data that has passed through all of the previous SIM phases. Visualization allows security personnel to quickly identify security threats and perform quick responses to those threats (netForensics, “Security Information Management”).

NetForensics Components

There are many components that make up netForensics. The netForensics components include:

1) SIM Desktop – The interface users interact with.
2) nF Web Server – Provides web publishing for netForensics.
3) nF Engine – Aggregates events.
4) nF Master – Provides real-time data from the netForensics Engine.
5) nF Provider – Provides netForensics reporting, configuration, and administration.
6) nF Agent – Provides communication for security devices (Cisco, “Understanding and Implementing netForensics”).

The following diagram from Cisco’s “Understanding and Implementing netForensics” shows how communication occurs between components in netForensics:

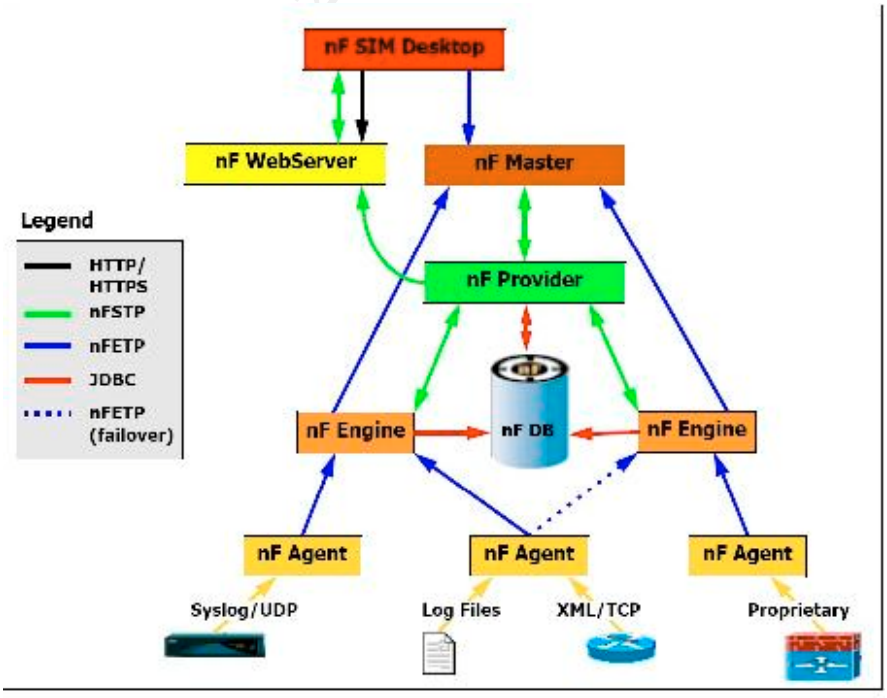

Figure 1: netForensics Architecture and Communication Hierarchy

What Gets Recorded
What does netForensics record from data that it collects? NetForensics records important details like the attacker source address, destination address, event severity, alarm ID (based on 150 events defined by netForensics), event category (type of event, for example Port Scan), timestamps, protocols, as well as many other details that may be useful in the identification and analysis of an attack.

Data Storage
So where does all the information go exactly? All of the data that is collected by netForensics is stored in an Oracle database on a dedicated netForensics server. The Database Server is not limited to only performing database tasks, but usually it is best to keep additional tasks on the database server to a minimum (Godfrey). Fewer additional tasks on the database server will help to maintain optimum performance. Another optimizing step is to use RAID storage, such as RAID 5+0.

How much data can I store exactly? There are no real limitations on how much historical data you can store using netForensics. The main question is how much disk space can you afford. With proper planning even the most active organization could house months of historical data. The best thing to do would be to have as much database storage space as possible.

How hard is the database to maintain? Not hard at all. NetForensics provides all of the tools that you need for automatically maintaining the netForensics database. This leaves security administrators with extra time for other things.

An Engine Drives It All
Now that you know where the data goes the next question is obvious. How does the data get there? NetForensics agents report to an engine that processes all of the data messages. Devices that have an installed netForensics "agent" transmit this data to the netForensics Engine using XML over TCP/IP. The netForensics Engine and Database communicate using Java Database Connectivity (JDBC). This may not be the most secure solution, but it does make things simpler. If secure communications are required there are additional options such as third party JDBC drivers, or the use of IPSEC at the host level (Godfrey).

Advantages
So what are the advantages? How about the elimination of manual monitoring each individual security device for starters? With netForensics software, security personnel are potentially able to view all security events for an organization from a single console. Monitoring is improved by netForensics capability to display automatically correlated security alerts in real-time.

NetForensics offers surprising ease of use. NetForensics features an easy to use web interface that can be run on Windows or Unix (Redhat or Solaris). The netForensics console can be run on as few or as many systems as your organization needs. The flexibility that netForensics offers with its web console allows for security administrators to access security alerts from home, or on a business trip (Taylor).

NetForensics offers scalability and flexibility. NetForensics software is scalable to meet the needs of virtually any organization (Comstor). NetForensics components can be run on one server, or many servers, depending on business size and security message load (Godfrey). NetForensics has been created so that many software parameters can be changed just by modifying the provided XML configuration code. This allows for great flexibility in configuring netForensics.

Reports and graphs can be easily generated. NetForensics offers a variety of customizable reports and graphs that can be scheduled and run whenever you like. Security administrators can have a customized report sent automatically to their email account at work or at home. Senior management can be also benefit from this and receive customized reports that fit their own needs.

Graphs are available in three ways in netForensics reports. The three graphs are columnar, bar graphs, and pie charts. Out of the box netForensics charts are very useful, but they could use a lot of tweaking for maximum usefulness (Godfrey). Specific reports are even available to find possible Worm activity (Cisilion).

NetForensics can notify you when events occur. NetForensics allows administrators to receive alerts via a pager or email whenever a particular attack is detected (Sturdevant). NetForensics allows security personnel to be notified of events no matter where they are.

Using NetForensics

How do I see attempted intrusions and security events in real-time? After accessing the netForensics web server you will navigate to the SIM Desktop. The SIM Desktop is an interface built entirely in Java. The SIM Desktop gives the user four customizable views, somewhat similar to the Linux X-Windows desktop. Each of these views can be saved so that when you log in everything will be arranged exactly how you like it. From here you can access any of netForensics useful tools. The most useful is most likely the real-time Event Console. NetForensics Event Console provides a real-time view of events as they happen, and it can be customized based on sensor and severity (Godfrey). This allows security personnel to filter out less important alerts so that they are not overwhelmed by too much data at one time (Godfrey).

NetForensics also has a Device Status View that allows users to view a real-time list of all devices and their alerts in an easy to read chart and graph. This view is useful for identifying which devices are sending the most alerts, and what categories the alerts are showing up in.

Can I share netForensics with non-security administrators or the Help Desk without giving them full access? Of course you can. Accounts can be created to give others the capability to view and query netForensics log information. This access can be shared with other administrators to increase their effectiveness in responding to network intrusions. Accounts can be given as little or as much access as you desire.

Product/Agent Support

NetForensics provides support for nearly all of the security industry's leading security software and device vendors. Whether you have a Symantec Enterprise Firewall, Netscreen Firewall, or a Snort Intrusion Detection System, netForensics most likely has the support that you need. Device support is available for Cisco Secure PIX, Check Point Firewall, Cisco IOS Firewall, Cisco Secure IDS, Cisco Secure PIX Firewalls, Cisco IOS IDS, Cisco VPN Concentrator, Entercept Host IDS, Cisco IOS Access Control Lists, ISS Real Secure IDS, Unix Syslogs, Windows NT/2000 Logs (Taylor), Dragon Sensors, and Snort (Godfrey). And if the device that you have does not currently have specific support, netForensics provides a Universal Agent that can be used with nearly any security device (Taylor). The Universal netForensics Agent requires a considerable amount of tuning and configuration, which may best be left to experienced security administrators.

Potential Impact

What affect will a SIM like netForensics have on my organization? A SIM solution will allow your organization to monitor more devices in less time than they can currently. Because of the increased monitoring capability, removal of redundant data, and normalized data a security team will be able to provide better, more reliable, security protection. A SIM solution will allow for a lower Total Cost of Ownership for security in an organization.

Do I Really Need All This?

Why do I need a SIM solution? Network security is an easy job, isn't it? Actually network security is a very demanding job. Network security involves 24 hour monitoring and response. Security teams are often overwhelmed by the amount of log data that is collected. This causes long response times to alerts, and quite often alerts that are completely overlooked. A SIM solution allows security personnel to better manage the overwhelming amount of alerts and messages at an organization. In addition, security personnel will have more time to notice and respond to unusual patterns that are not normally detected that may have otherwise gone unnoticed. NetForensics provides a central point of management for all of your network security needs (Godfrey).

Pricing
A SIM product like netForensics does not come cheap. NetForensics is competitively priced though, usually around $60,000 (Sturdevant). More basic packages are available for smaller businesses at considerably lower prices. For a business that has a considerable amount of security data a SIM solution can easily pay for itself because it can allow you to monitor more equipment with fewer personnel.

Support
NetForensics offers product support from 7am to 10pm Eastern Time, Monday thru Friday, which is pretty impressive, but could be improved upon. For a product as critical as this one I would prefer 24 hour, 7 day a week support.

NetForensics support line is friendly, and responsive to any issues that may occur. My experience with them has been good, other than a few times when my open trouble calls were closed without resolution and without netForensics support contacting me. When I called back however, netForensics support personnel were more than happy to re-open my trouble call.

NetForensics also offers a support website with known issues and problem resolutions. Access to the netForensics support website is restricted to their customers. The netForensics support website offers quite a bit of good information, but for many of the technical problems I have encountered there were no previously documented occurrences.

On-site installation and support is available for businesses with money to spare. I found netForensics on-site personnel to be exceptionally knowledgeable and flexible. If you have paid for additional support time netForensics will also provide you with the training you need to operate netForensics, and even how to set up the software on your own.

NetForensics software is mildly deficient as far as documentation goes. When I received my software package all I got was a small plastic case with the software and an electronic copy of the supporting documentation. The documentation that is provided is sufficient to install the software in most cases, however for me it does not provide quite enough useful technical details about the specifics of how the software works. The documentation provided by netForensics also does not provide any troubleshooting measures that I was able to find useful. If something goes wrong during the installation, plan on calling netForensics technical support.

Software patches are available through netForensics, and are provided with your support contract. Each patch has supporting documentation that details step-by-step how to install the patch. Most patching is as simple as copying a file to the netForensics Provider Server and running a patch installation program.

What Problems Did You Encounter?
My experiences with netForensics have been relatively trouble-free with a few exceptions:

The first problem I encountered was immediately after installation. The automatically generated reports had web links to non-existent files on the netForensics server. Due to our multi-server configuration the generated report was looking for the images on the wrong server.

The second problem was a little more severe and complex. The netForensics agent for the Symantec Enterprise Firewall repeatedly locked up the firewall during log rollovers. Finding the cause of this problem required sending many logs to netForensics support via email. The problem was that we were allowing the firewall logs to rollover time-based as well as size-based manner, and the original version of the agent only allowed for one or the other. Fixing this problem was very time consuming, however netForensics graciously updated the agent to allow for both types of log rollovers.

The last problem that was encountered was a failure of the web server. This was more of a mistake than anything. The cause was incorrectly booting the netForensics server that hosted the Web Server and Engine before the netForensics Provider Server. There was no provided documentation that I am aware of that specified the order to boot the servers in, however the boot order does make sense. Considering the complexity of the netForensics deployment, I consider these problems minimal.

Ease of Installation
Can I install and configure netForensics alone? Probably not. NetForensics requires an extensive amount of tuning and configuration and may require the assistance of a consulting company (Sturdevant). On the bright side, agent installation for supported devices is a snap with easy to use installation wizards.

Were there installation considerations that netForensics failed to mention? Yes, there may be an increased load on servers and other systems that are running netForensics agents. You may want to reconsider agent installation on systems that are already under a considerable resource strain, particularly processor consumption. Another important consideration is increased strain on network resources. On servers that already have a high network load you may want to consider adding an additional network interface card to manage the additional network traffic.

Conclusion
NetForensics has done an excellent job of providing an easy to use security management package. From netForensics easy to use interface to its unlimited scalability, netForensics software offers a well thought out solution to some of the problems facing security professionals today.

NetForensics will also work with you to ensure that your product works like it is expected. Is netForensics a perfect solution? Not yet. But right now they are the leader in SIM solutions, and they are well on their way to being that perfect solution (Shipley).

References

"Case Study – Empire Blue Cross Blue Shield." Comstor. 2003. Comstor. 15 Dec. 2003 <www.comstor.com/visitor/hipaa/pdf/casestudies/netforensics/Blue_Cross_Blue_Shield.pdf>.

"Correlation – A Two-Tired Approach." NetForensics. 2002. NetForensics Inc. 15 Dec. 2003 <http://www.netforensics.com/ciscomicrosite/documents/nf%20comprehensive%20correlation.pdf>.

Godfrey, Michael. "NetForensics – A Security Information Management Solution." SANS. 2002. SANS Institute. 15 Dec. 2003 <www.sans.org/rr/papers/61/408.pdf>.

"NetForensics." Cisilion. 2003. Cisilion Limited. 15 Dec. 2003. <http://www.cisilion.com/netforensics-why.htm>.

"Real-Time Correlation – Statistical Correlation Through System Scoring." NetForensics. 2002. NetForensics Inc. 15 Dec. 2003 <http://www.netforensics.com/ciscomicrosite/documents/nf%20realtime%20correlation.pdf>.

"Security Information Management – A Solution to Enterprise Security Management." NetForensics. 2002. NetForensics Inc. 15 Dec. 2003 <http://www.netforensics.com/ciscomicrosite/documents/sim%20strategies.pdf>.

Shipley, Greg. "Security Information Management Tools: NetForensics Leads a Weary Fleet." Network Computing. 2003. CMP United Business Media. 15 Dec. 2003 <http://www.networkcomputing.com/1307/1307f2.html>.

Sturdevant, Cameron. "NetForensics Effectively Handles Hacks." eWeek. 2002. eWeek. 15 Dec. 2003 <http://www.eweek.com/article2/0,3959,741464,00.asp>.

Taylor, Laura. "NetForensics Brings It All Together." Advisor. 2002. Advisor Media. 15 Dec. 2003 <http://securityadvisor.info/doc/08556>.

"Understanding and Implementing netForensics." Cisco. 2003. Cisco Systems, Inc. 15 Dec. 2003 <http://www.cisco.com/application/pdf/en/us/guest/products/ps5209/c1626/ccmigration_09186a008017e180.pdf>.