Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Log Management SIMetry: A Step by Step Guide to Selecting the Correct Solution

nd logs requiring a significant time investment to properly address important issues. As compliance, incident response and an increasing demand for IT security efficiency become more prevalent, organizations struggle with how to manage these disparate technologies efficiently and effectively. This is where a security information and event management system can help solve some of those challenges. ...

Copyright SANS Institute
Author Retains Full Rights

AD

Log Management SIMetry: A Step by Step Guide to Selecting the Correct Solution

GSEC Gold Certification

Author: Jim Beechey, beechey@northwood.edu

Adviser: Jim Purcell

Accepted: October 21, 2007

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. Introduction.....3
2. Determining Organizational Requirements.....7
3. List Log Genterating Devies.....12
4. System Sizing.....17
5. Key Differentiators.....22
6. Choosing Your Solution.....29
7. References.....34
8. Appendix A.....35
9. Appendix B.....36

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

The information security profession continues to evolve and advance as organizations place greater value on their information security programs. These programs have grown significantly in the past few years, especially in small to medium sized organizations. Technical solutions such as: firewalls, VPNs, antivirus, patch management systems, intrusion detection/preventions systems and vulnerability scanners have all helped to address specific security issues. These technologies have also created a mountain of alerts and logs requiring a significant time investment to properly address important issues. As compliance, incident response and an increasing demand for IT security efficiency become more prevalent, organizations struggle with how to manage these disparate technologies efficiently and effectively. This is where a security information and event management system can help solve some of those challenges.

The terms SIM (security information management), SEM (security event management), SIEM (security information and event management) are all typically used to describe the same general solution. For the purposes of this paper we will refer to all such systems as a SIM. A SIM can be separated into four functional areas. First, a SIM collects and stores logs from network devices, security devices/applications and host operating systems/applications. Second, a SIM correlates logs from various sources and produces alerts regarding important security issues. Third, a SIM typically provides a ticketing system or automated remediation options used to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

address and resolve security alerts. Fourth, a SIM provides a reporting mechanism for compliance, auditing and security monitoring.

If supported, a SIM can collect and correlate logs from just about any device or application in your network. Examples include routers, switches, wireless access points, firewalls, IDS/IPS, NBAD (Network Behavioral Anomaly Detection) devices, vulnerability scanners, windows hosts, unix hosts, services such as DHCP or DNS, authentication services such as Active Directory, Radius, and LDAP as well as applications such as Apache, Exchange and antivirus software. Log collection is most often accomplished with redirecting syslog output to the SIM, but can also be accomplished with vendor specific methods such as Checkpoint's LEA.

Once logs are collected, the true power of a SIM becomes evident. Imagine the following example of what would happen when an exploit is attempted in your network with and without a SIM in production. Without a SIM in place your IDS would fire any number of times alerting you to the fact that a known exploit was attempted against a specific IP address in the organization. You or your staff would need to look into the issue to determine its relevance and effect. With a SIM in place you would receive a prioritized alerts based upon not only the exploit, but the targeted host, its vulnerability state and actions occurring due to the exploit. For instance, the following would produce a very high priority event: a windows server 2003 exploit was detected; it was run against a windows 2003 server; according to the latest vulnerability scan that server has not yet been patched and the server reports a new service

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

was just started. YIKES!! Clearly you have a major issue that needs immediate attention. Based upon the prioritized alert a ticket would be generated so that whoever is responding to the incident can document their steps to remediation. In the weeks and months that follow this incident, the SIM would allow the security staff to report to management or auditors regarding the effectiveness of your security operation.

The SIM market today is a very crowded and complex place as you can see by the vendor list in Appendix A. Not only are there many solutions out there, but since one of the major components of a SIM is third party device/application integration, there are major differences in product support between the various solutions. Also, different solutions fit different needs. Some are better positioned for compliance while others are more suited toward incident response. These market characteristics make it very difficult to say product X is better then product Y, but rather, make product selection highly dependant upon your organizational needs. One size does NOT fit all. Gartner's report states this best: "…organizations may need to evaluate offerings from vendors in all quadrants, depending on their requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of security information management (SIM) and security event management (SEM) capabilities, ease and speed of deployment, the IT organization's support capabilities, and integration with existing network, security and infrastructure management applications." (Nicolett & Kavanagh, 2007)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

For those considering a SIM solution, I offer one general word of caution. While the benefits of a properly tuned SIM are very clear, the process takes a significant investment of both time and money. Be prepared for lots of research and testing before you begin the implementation process. This industry changes rapidly, therefore I recommend making this process a priority rather than something to review as time permits. Also, if your organization doesn't yet have in place some of the key security technologies such as an IDS/IPS and vulnerability scanning solution; then implement and properly tune those devices first. A successful SIM is only as good as the alerts it receives from the various devices.

The ultimate goal of this paper is simple: help you choose the correct SIM solution for your organization. This paper is not meant to be a comparison of specific offerings of one company or another, but rather a guide to help you through the selection process. Generally, this paper should be helpful to all sized organizations, but is specifically targeted towards small to medium organizations which may not have the resources of their larger counterparts. In Appendix B there are templates designed to be filled out by your organization during the product selection process. I recommend first reading through this paper and then completing the templates. Refer back to the paper as needed when questions arise. So, without further ado, let's get started!

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2. Determining Organizational Requirements

As you begin the journey into the world of SIM, resist the temptation to start doing extensive research on various companies and their solutions. There will be plenty of time for that as we move forward. While the upcoming process can seem a bit mundane, having a clear picture of your organizational requirements will save you significant time when it comes to choosing the vendors you want to focus on and in the end, make a more informed decision for your organization. "…log and data transportation, storage, reporting, monitoring and forensic analysis are all part of a complete SIM effort, so make sure you understand which elements are the most important to you and know which vendors can deliver. And despite what vendors say, there's a lot more to security log and information management than deploying an appliance. A sound strategy and upfront planning are just as critical." (Shipley 2007) The following steps explain in more detail the questions asked in the SIM Organizational Requirements Template located in Appendix B.

STEP 1

First, and foremost, what is the overall reason for pursuing a SIM solution? This can make a huge difference in the type of solution you should pursue, especially if a specific compliance driver is the issue. Since there is likely more than one reason, please rank from 1 to 4 with 1 being the most important. Compliance refers to a specific government or industry regulation whose standards your company must meet. Log aggregation refers to the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

process of collecting logs from many different devices and systems into a central location. Incident Response refers to the process by which attacks against your technological assets are identified, remediated and prevented. Increased security efficiency refers to using technology to perform tasks previously performed by a person.

STEP 2

If compliance is one of the key drivers of your project, please identify the regulation your organization must comply with. Examples include the Payment Card Industry Standard (PCI) for organizations accepting credit card payments, Health Insurance Portability and Accountability Act (HIPAA) for health care providers, Gramm, Leach, Bliley (GLB) for financial institutions and Sarbanes-Oxley (SOX) for publicly traded companies, This will help focus your efforts and those of the vendors who will be discussing various solutions.

STEP 3

Consider your internal support options for your SIM solution. While most companies offer appliance based solutions, some do not and can require significant back-end expertise. For instance, is your IT group prepared to support a SIM which requires Oracle database administration knowledge? This can be an especially important issue for the SMB market. This issue here is should solutions which are NOT appliances even be considered.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

STEP 4

Log collection for those devices which do not natively support syslog, especially windows boxes, can be one of the big challenges in a SIM solution. Depending upon the organization, installing agent software, especially on servers, can be no big deal or require an act of congress. If your organization requires agent-less solutions you will limit your choices, but it's certainly better to save yourself some time upfront. Remember though, we are talking about a requirement, not a preference. Don't limit your choices based upon this factor unless agent based solutions are truly not an option.

STEP 5

Does your organization require that you maintain logs in their raw format? Raw logs are simply the logs from various devices in their original format. Normalized logs have been converted into a different format for data presentation or storage needs. Raw log access might be necessary for forensic or legal purposes depending upon your organizational stance. Check your security policy or with legal council to determine your requirements. "With early SIM products, the raw log files were altered to facilitate insertion into a database and provide data reduction; this optimized the use of space. It was important when SIM first hit the market 5 or so years ago, as the technology was not fast enough to store all the data in a forensically clean way, and the problem being addressed was event correlation, as opposed to compliance or forensics. Ergo, the emergence of log management products. These purpose-built boxes quickly gather log data from a variety of different devices, and they

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

do so in a forensically clean way, maintaining the integrity of the data, so it can be easily analyzed for forensics and compliance purposes, although not necessarily for real-time management. This log management data, though, will hold up in a court of law." (Rothman, 2007) In general, SIM solutions will either lean towards real-time alerting or log management. However, the good news is that these lines are becoming more blurry and many of today's systems keep logs in both normalized and raw format, thus attempting to meet the needs of customers looking for both real-time alerting and log management capabilities.

STEP 6

How long should logs be stored before being deleted? Of the questions asked in this section, I find this to be one of the most difficult for many organizations to answer. Often competing interests can be at work in determining the appropriate timeframe if an organizational or compliance mandate does not exist. Legal experts typically prefer as little log retention as possible, where as operational staff often prefer to maximize log storage timeframes. If you don't have a policy on this subject, take the time to gather the appropriate people together and come to some kind of consensus on the issue, especially if your operational staff intend on utilizing the SIM for non-security related purposes.

STEP 7

Network Behavior Anomaly Detection (NBAD) is technology which analyses network flow logs to determine when malicious and/or

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

anomalous traffic is traversing a network. “With NBAD, security professionals are not exclusively looking in the rear view mirror, trying to figure out a disaster that's already happened. Because of the technology's faster reaction times, network behavior anomaly detection is poised to break out in 2007, especially if it's integrated with the SIM software sitting on your shelf.” (Rothman, 2007) NBAD can impact your SIM selection in several ways. The SIM Organizational Requirements document lists three options to consider. First, there are a couple solutions that offer NBAD as an integrated part of a SIM solution. These can be an ideal fit for an organization without an existing NBAD solution who want to analyze network flow data as well as device logs; however, selecting this choice will severely limit your vendor choices. A more likely option for most organizations would be to selection option 2, a plus, but not required. If you already have an existing NBAD product in production you would certainly want a SIM solution that supports your existing solution. Marrying network flow data with server/device logs can significantly increase the effectiveness of your SIM solution. Integrating NBAD provides another view into your network that you just can’t get from any other source.

STEP 8

Automated remediation options are somewhat of a niche area in the SIM market. Several companies offer such solutions, but with varied implementations. Automated remediation involves integrating various devices into the SIM so that given certain occurrences a device could be blocked, quarantined or removed from the network

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

altogether. The most common method for doing so would be to integrate with a firewall or router to automate the writing of a blocking rule or ACL for an offending device. Implementing automated remediation sounds like a great idea, but can have major pitfalls. These solutions must be tuned very carefully to ensure that false positives do not create havoc on your network.

STEP 9

SIM solutions are typically focused on network and server resources and not end user workstations, however log collection from these devices is possible and even a strength of certain vendors. Often the biggest barrier to log collection from individual workstations is this dramatically increases device count which is often a metric used to determine licensing costs. Also, if considering log collection from workstations, give strong consideration to the method of collection on Windows operating systems. This topic will be discussed in detail in a later section.

3. List Log Generating Devices

The following section is dedicated to listing out your organizational assets that you would want a SIM solution to support. List all devices in your organization, even those you might not send logs from initially. You never know when the need will arise to collect logs from a given device and it's best to understand now what devices are supported and which are not. Device support typically means that the SIM solution can accept or gather logs from the particular device, interpret them and correlate them against the

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

system's rule base.

This section is divided into functional areas of devices most commonly sent to a SIM. Vendors will often list product support in similar subsections. Each subsection has a table for noting the product's manufacturer, product, version and, if applicable, quantity. Noting the version number is probably the most time consuming piece to this exercise, but also the most valuable. What good is support for your IDS if the SIM supports version 1 and you're running version 11, which by the way has a completely different log structure. Quantity is important, as it will determine the maximum number of devices the SIM will need to support. Again, list all devices even if you don't intend on supporting all of them. Your initial numbers should be based on "highest possible" scenario.

STEP 10

This step simply asks you to list the antivirus and, if different, antispyware software used within the organization.

STEP 11

Listing authentication sources on the network can be a little more complex as initially thought as there may be several sources in your organization. Options may include directories such as Active Directory, Novell, LDAP as well as proxy type solutions such as RADIUS or system specific authentication such as local accounts on a large Unix system or database application. Make sure that all login points in your organization are covered based upon the technologies

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

and vendors listed. If you have multiple implementations of the same standard such as Microsoft's Radius and Juniper's Steel Belted product, list them both. Think about options such as internal workstation authentication, wireless, SSL/IPSEC VPNs, dialup and even two-factor systems such as RSA SecureID. Determining who is logged into a system at a particular time is certainly one of the key aspects an SIM can provide; therefore authentication support is a big piece to the puzzle.

STEP 12

This step asks you to list the DHCP servers used within the organization and should be a fairly straightforward process.

STEP 13

List any NAC (Network Access Control) solution in use within the organization. NAC solutions are used to control device access to enterprise networks. A NAC solution can provide a combination of options including authentication prior to access, end point security checks, traffic policies and traffic monitoring. The goal is to only allow network access for those people who should have it and those devices who meet the organizations security policy. The authentication data and often DHCP services are very relevant to a SIM deployment.

STEP 14

Many organizations have already setup centralized management and logging systems for one, if not several, of their technology areas.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Examples of such systems relevant to a SIM implementation would be Microsoft Operations Manager (MOM), IBM SiteProtector and Juniper Network Security Manager. If supported, your SIM solution could collect logs from the management system rather than having the originating device send its logs twice over the wire. This can help save on bandwidth and system performance, especially in situations where devices are sending their logs across lower speed WAN or VPN connections. SIM access to these systems typically happens in one of two ways; either the SIM can query the logging system's database directly or the logging system can be setup to redirect or export logs to the SIM.

STEP 15

List all server operating systems used within the organization. Please include specific details regarding various flavors of Unix and Linux as there can be varying levels of support in these areas.

STEP 16

List key applications used within the organization. Examples would be items such as Exchange, IIS, SQL, Oracle and DB2. No SIM vendor is likely to support all your internal applications; however the more complete list the better.

STEP 17

List vulnerability scanning tools used within the organization. Vulnerability scanning systems can add an additional layer of insight into a SIM solution by providing asset information and details

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

regarding vulnerabilities that may exist on that asset. Vendor support for these solutions can vary greatly between vendors. For instance, when we were going through our evaluation process, two of our finalists supported our vulnerability scanner. One could import the xml data file the scanner produced, while the other could log in to our solution, schedule a scan and automatically import the results. Cleary, this was a huge difference in the level of support even though both were “supported”.

STEP 18

List firewall and intrusion detection/prevention devices used within your organization. These devices are some of the most critical components of a SIM solution and support for these devices is a must. The good news is that most vendors have support for numerous solutions in these areas.

STEP 19

List any VPNs used within the organization whether they are client based, such as IPSEC, or SSL based. Keeping tabs or your remote users and entry points into the network is certainly something that is very important to most organizations.

STEPS 20-22

These steps are fairly self explanatory and require little explanation. Generally, routers, switches and wireless access points will be secondary to other devices in your SIM solution, but still can provide some useful information. Make sure to list any devices

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

we've missed in the previous steps.

4. System Sizing

Now that organizational requirements and log generating devices have been determined, the focus turns to properly sizing a system. Vendors have a myriad of options when it comes to various system sizes and models. However, a few consistent metrics such as device count, events per second and storage requirements can be applied to nearly all solutions.

DEVICE COUNT

Device count is the easiest of the three to determine. Simply count the total number of devices you expect to be sending logs to the SIM. For the purposes of an evaluation, use the total number of devices developed in the previous section. Make sure though you decide whether or not you'll be including workstations as they can have a significant impact on the total.

EVENTS PER SECOND

Events per second (EPS) is probably the most consistent metric used across vendors. EPS is the number of log messages a system can receive in a second. The number of EPS can become very large, very quickly, considering the types of devices that integrate into a SIM. Firewalls, for instance, produce large log volumes as each and every incoming or outgoing connection creates a log event. Considering a single web page will produce several connections, it is easy to see

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

how the numbers can grow quickly. At first glance, determining your organization's EPS can be one of the more daunting tasks in selecting a SIM. However, with a few quick tricks and a little setup time, an organization can fairly easily get an accurate picture of their requirements.

When determining EPS, there are really two general approaches to take: either collect logs from all devices or collect logs from a single device of a given family and estimate the total. Both approaches are fine, the correct method depends on your timeframe and need for exactness. If you choose to estimate EPS, make sure that you only do so for similar devices. There can be a great difference in the log volume between dissimilar devices. For instance, during our evaluation certain windows servers produced 30 times the log volume of other servers.

The vast majority of devices you'll integrate into a SIM will send their logs via syslog; therefore the first step in determining organizational EPS is to setup a syslog server and point network devices at it. There are numerous syslog servers for both Windows and Linux operating systems so feel free to use whatever tool you are most comfortable. For those new to syslog and more experienced with Windows than UNIX, I suggest using Kiwi Syslog Daemon for Windows from Kiwi Enterprises. Kiwi is recommended because it runs on Windows, is easy to install, shows incoming syslog messages in real time, has syslog traffic statistics and is free. Kiwi even has the capability of emailing daily syslog traffic statistics which is perfect for our needs.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Once Kiwi or a similar syslog product has been setup, begin configuring devices in the network to point to the syslog server. Most network devices and Linux/Unix hosts have configuration options for directing device logs to a syslog server. Check with the manufacturer's documentation for specific configuration details. Also, make sure that the device is configured to log everything required in the organization. Remember, this exercise is looking to get a baseline for how many events per second the SIM must support. Therefore, I recommend turning on as much logging as possible so that the estimate created will be on the high side. If a firewall resides between your device and syslog server, make sure the port 514 UDP is open between the device and the server. As you turn on syslog for a given device, check to make sure the logs are arriving at the syslog server by watching the real time monitor Kiwi provides.

Determining events per second for Windows servers and hosts bring an additional challenge as Windows does not support syslog natively. However, there are several options. If your organization is already collecting Windows server logs centrally, see if there is some kind of report or statistics available to determine how many log entries per second are being generated. If not, you could estimate the number of log entries manually. Simply connect using Windows event viewer to various server types throughout your organization and calculate how many log entries per second are generated. A third, more precise option, is to install an application such as SNARE on various Windows boxes. SNARE takes windows event logs and converts them to syslog output. This output could then be directed at your existing syslog server used to determine EPS for your network

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

devices. Using one or a combination of the above methods should provide an accurate picture as to the number of events per second an organization's server infrastructure is producing.

In order to develop a clear picture of the organization's log volume I would recommend collecting logs for a minimum of one week. This will give the opportunity to see general trends due to time of day, weekends, etc. While going through the process to determine EPS there are a few key things to remember. First of all, the number does not have to be perfect. Vendors will provision a solution in large ranges, therefore numbers to do not have to be precise, just make sure to round up and add appropriate capacity for growth. Second, spend a good amount of time considering the usage patterns of your organization. Vendors do not typically take an average over a period of time, but rather the solution is licensed to a maximum threshold. Therefore, your average EPS during peak usage is really the key mark in determining what volume your SIM needs to meet.

Storage requirements can be determined several ways, but in general terms you want to multiply the storage size of a full days worth of logs by the number of days you want to store log files. If you collected logs using Kiwi or some other syslog tool to determine your organizations EPS then you likely already have storage requirements determined. Kiwi and several other syslog tools will collect all logs to a single file for each day of the week, therefore making it very easy to calculate a daily size for all your log files. If you are estimating log size; determine an average syslog message size, multiply by your EPS, then by 3600 (seconds in a day). Next

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

convert the total from bytes to gigabytes and multiply by the number of days you wish to store logs for. Many vendor solutions are capable of compressing log files which will help with storage requirements. However, for planning purposes, I don't like to take compression into the equation. Extra cushion is always a good thing when planning for disk storage.

System sizing for non-appliance based solutions is, of course, a completely different ballgame. The same metrics apply and may need to be determined; however the manufacturer's recommendations for hardware specifications should be your guide when making purchasing decisions. The data collected will still be needed by the vendor; however they should be able to tell you what your server(s) requirements are.

VENDOR DEFINED SIZING

The marketplace has one additional hardware sizing model which is worth some discussion time. I call it the "tell us what you have and we'll size your solution" aka "smoke and mirrors". There are vendors who will take the approach of having a customer provide them with a list of products they wish to collect logs from and then design a solution for you. There typically is no discussion of metrics such as events per second. You'll hear things like "Our engineers are experts and do this every day" and "sizing based on events per second is dangerous". In my opinion, allowing a vendor to determine an appropriately sized system for you without proper internal scrutiny is considerably more dangerous. Consider the following example; our organization has approximately 30 firewalls.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Three larger firewalls located at our three main locations and 27 others at smaller remote sites. The vendor hears 30 firewalls and thinks our log volume is going to be through the roof, when in fact the vast majority of these firewalls serve very small offices containing 5 or less employees. In fact, our total events per second are quite reasonable. When I discussed this issue with our rep I was completely stonewalled. They could not give me any data regarding the performance of the box they were quoting. My point here is not to bash any particular vendor or model, but rather to underscore the importance of digging into this process and to not let a vendor lead you blindly to a given solution.

5. Key Differentiators

Shortly, we will be looking at specific vendor solutions. How do we narrow the field down and begin choosing our solution? In any evaluation there are certain key factors which separate one solution from another. Of course, these can be very different depending upon the organization; however I believe a few key issues will help most evaluations. As you are going through the process, make your own list of key differentiators. This information will be very helpful during the evaluation process and make sure you get the most out of your dealings with vendor sales and technical staff.

FIREWALL AND INTRUSTION PREVENTION/DETECTION SUPPORT

Any solution which does not support your organizations firewalls and intrusion detection/prevention systems should not be considered. These devices are the basis for an organizations network security and

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

support is simply a must.

SERVER OS SUPPORT

Does a solution support the servers deployed in your organizations? This is especially important for those shops running Novell as support appears to be limited. Linux/Unix support is typically available, but there may be caveats as to support beyond login/logoff activity. As expected, support for Microsoft Windows servers is built into nearly every system; however, how this support is implemented is key to the selection process. Windows does not support syslog natively; therefore most systems require one of the three following options: the snare client, a proprietary client or agent less log pulls. Let’s take a closer look at each of these options.

The snare client is used by many SIM vendors to collect Windows server logs. Snare is an open source product which converts windows event log data into syslog output. Snare has the advantage of being widely used and, being open source, is free. Unfortunately, some may be leery about relying on an open source product for enterprise log collection. When issues arise, who do you go to for support and will the SIM vendor fully support snare?

A proprietary client is another option for Windows log collection. Typically a vendor decides to write their own agent to avoid the concerns and issues involved with SNARE. Often these clients continue the same process of converting windows event logs into syslog output. Proprietary clients have the advantage of

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

providing one source to go to for support issues. However, they still require the installation of additional software into an organizations server infrastructure.

Clientless log pulls is the third option in this discussion. At first glance this option seems to be the clear winner. Who wouldn't want agent less log pulls? No software to install and shorter implementation times. Of course, clientless agent pulls have their disadvantages as well. Typically, clientless agent pulls are usually only available on SIM solutions which run Windows themselves, which can severely narrow the options available. Also, scalability can become a concern in this configuration as logs are pulled using NetBIOS. This can be very system intensive for large log volumes and slow across WAN connections.

There is no definitive answer to this Windows logging dilemma. However, with careful thought, testing and discussion your organization can make the correct decision regarding Windows logging.

LOG COLLECTION AND MANAGEMENT

At its base, SIM starts with simply collecting logs from a variety of sources and, yet, there still can be very different options, even in this area. One key issue for many organizations, especially those who expect to have this tool help with forensics, is the availability of logs in their raw format. Raw format refers to the log file in its original state. Most SIM solutions will normalize logs from their original state for correlation and storage purposes. Another similar issue to consider is what options are

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

there for exporting logs and, if available, what format are the logs exported to? Think about situations where you may need to provide log data to another system, department or group. Will the SIM meet these needs?

Backup and restore is another log management issue to address during your evaluation. Needless to say, your SIM solution will require large amounts of data. What are your requirements to backup and restore this data? Many SIM systems run on very proprietary backend databases. Is there an efficient method for performing backups and restores? How long do you want to keep a copy of your logs and in what format?

When doing system evaluations take a close look at what options a user has for searching through events. Some vendors will limit your ability to customize searches in order to gain efficiency and performance. Make sure that your search needs will be met.

RULES

Rules are the basis for how logs are correlated into an incident or offense. When evaluating SIM solutions you should consider three main issues relating to rules: the number of vendor provided rules, the quality of these rules and capabilities for creating custom rules. Every vendor will provide a certain subset of pre-defined rules. The number of rules and their capabilities will vary greatly so take a good look when comparing solutions. For example, it is pretty easy for a vendor to write a rule looking for failed authentication attempts. However, a much more involved and useful

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

rule might look for failed login attempts spread out over a long period of time, across several systems, from a similar source address.

Pre-defined rules are important, but I believe the ability to create custom rules is even more important. No organization has the same assets or security needs, therefore the ability to create rules specific to your organization's needs is important. Try creating a custom rule and see how easy the process is and if the interface limits your choices. All vendors will say you have the ability to create custom rules, but what does that really mean? Can you completely define the parameters of your rule or are you limited by their predefined templates? Do you need to be a programmer to write effective rules or is there an easy to learn system?

INCIDENT MANAGEMENT

Once an alert has been generated for a particular issue, the responding individual will begin the organization's incident response process. SIM systems often include some form of incident or ticket management system to aid in this process. Typically these systems are much more limited in scope than full blown Help Desk software; however they can still be very useful in organizing and prioritizing alerts and documenting your response. Larger organizations may also wish to look at options for integrating alerts from the SIM into their existing Incident Management System. During your evaluation, think about the process you will follow to take an alert through the incident response process and how your SIM can assist in this process.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

REPORTING

Reporting is a key differentiator for many SIM decisions, especially with compliance often being a key reason for pursuing SIM. “Compliance has become the principal driver in the deployment of SIM technologies, says Scott Crawford, a senior analyst in the Enterprise Management Associates security and risk management group. Whether it's to meet regulatory standards or merely to satisfy internal policies, enterprises have expanded their use of SIM tools to embrace what is increasingly called governance/risk/compliance (GRC) management, he explains.” (Carr 2007) All vendors will say their solution can solve all our compliance needs, but as with all vendor claims; test, test, test. SOX, HIPAA and GLB related compliance reporting get all the hype when it comes to a SIM, but consider how you could use the SIM for your operational reporting requirements as well. For instance, we are using our SIM to develop web-based dashboard to track usage of various IT systems across our organization.

Evaluating a reporting solution is very similar to evaluating rules. All systems come with certain predefined reports and typically a method for creating a custom report. Make sure and test custom report creation during your evaluation. Think about the presentation of these reports both in paper and electronic format. Imagine if you had all this data in one location and were not able to appropriately report back to senior management. Also, SIM solutions can cost significant dollars, and upper management may be skeptical of the purchase, especially in smaller organizations. Proper follow

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

up via reporting will help justify the purchase and make future budget proposals that much easier.

COMPANY STABILITY

As mentioned above, the SIM market is a very crowded place which most agree is ripe for continued consolidation. Larger security companies without a SIM solution or looking to improve their existing product may decide that purchasing one of the smaller vendors is a better idea than developing their own solution. “But that was before big vendors began buying their way in the market, snapping up smaller SIM tools vendors left and right. Major SIM deals have included EMC’s September acquisition of Network Intelligence, IBM’s purchase of Consul and Micromuse, and Novell’s buyout of eSecurity.” (McLaughlin, 2007) The risks of purchasing a product who later is bought by a larger company are fairly straightforward; worries about continued support, migration paths, increased maintenance costs, degrading customer service. One of the more complicated and potentially dangerous issues is your deployed ruleset. As stated by Mark Bruck, president of BAI Security, “You can invest a lot or resources and time into tweaking the systems and developing rules around correlating events and triggers for specific types of events, but after an acquisition, all this work can go down the drain because there aren’t always clear migration paths from one vendor to another, and your system may not be as functional”. (McLaughlin, 2007)

The point to this section is not to scare you away from smaller company offerings, but rather to make sure that you understand the risks involved with the marketplace. Smaller companies can have

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

several benefits as well such as more personalized service, increased flexibility and potentially less costly solutions. The key is to understand the risks in the marketplace, your organization's tolerance for such risks and make the correct decision.

6. Choosing Your Solution

Up until this point, there has been no need to begin working on researching specific vendors and solutions. In fact, I highly recommend spending the time to determine your organizational requirements before talking to any vendors. However, the time has come to begin researching options.

As we begin the vendor contact and research phase, organizations will take different approaches based upon their purchasing requirements and past experiences. Some may choose to issue an RFP while others may choose a more informal evaluation process. Regardless of the direction of the evaluation and purchasing process, the steps above and advice below should be valuable regardless of approach. Appendix A provides a list of SIM products and vendor websites. This list is a good starting point for your vendor research.

I recommend spending a few hours going through this list and getting a feel for various offerings and their appropriateness for your organization. Let your requirements document be your guide in this process. Look for and read current reviews of SIM products. Let me stress the need for current reviews as older reviews can quickly become out of date as vendors are constantly changing and

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

evolving their product offerings. If available, take a look at current industry analyst reports. As you research various vendors and solutions, highlight those that interest you most and cross out those which are clearly not a good fit for your organization. Use your organizations most important criteria in doing this high level evaluation. Some vendors will have detailed information regarding their products and some will not, but you can still get quite a bit of valuable information without even contacting sales representatives. Pay close attention to those solutions which have lists of their support products online and, if possible, get a feeling for cost in relation to your budget. The goal should be to pare down the list to around five solutions.

After narrowing down the field, it's time to start contacting vendors. This portion of the selection process was the most bizarre I've ever been though. The methods for guiding customers the selection process varied greatly between companies. One vendor came onsite with an engineer, showed us the system, had a demo unit to us within two weeks and followed up with another on site visit just to help us get the system configured properly. Another vendor in our top five wouldn't even let us talk to an engineer without basically guaranteeing a purchase. We saw these two extreme approaches and just about everything in between. This market is very crowded, but clearly vendors are also very strapped for time. I believe it's important to make sure that whomever your contacting understands that your inquiry is serious and a defined objective for your organization. Now, having said that, don't give away key negotiating tactics such as your bottom line budget, but make sure whomever

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

you're contacting knows that you are serious about purchasing a SIM.

When contacting the first round of vendors, I prefer to get two key pieces of data. Determine their level of support for your organizations devices and get a ballpark idea on cost. Send them all or part of your organizational requirements document, especially if their supported product list is not online. Let them do some of the research for you. Your document will also show them how serious you are about pursuing SIM. Remember, when looking at supported products lists, make sure they are specific about not only the company and model, but also version they support. You may also choose to do some online demos to get a better feel for the systems. After you gather more detailed information, see if you can narrow the field down to three vendors. Price can become a key issue here as you begin to understand the high costs of certain systems. If you find yourself with limited options after getting ballpark figures, you may need to go back to your original list and contact other vendors.

At this point, it's time to get serious about the details of the systems you're looking at. Let your vendors know they are in the top three; they'll likely throw more resources at you. The time has come to get official quotes. Make sure these quotes contain maintenance costs as well as any additional hardware or software licenses that are needed. While we did not, many organizations will want to contract for professional services to help get them up and running quickly so be sure to include these costs if appropriate. Another key component to understand at this point is how the company handles system replacements. Meaning, in four years, your appliance may be

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

at the end of its useful life. What happens then? This is a very important item in determining your overall cost of ownership.

If support is lacking for one or two of your key organizational devices, you may be able to negotiate with the vendor to make adding support for those devices a part of the purchase. Try to get a feel for how they handle support for new and updated devices and ask for some concrete examples. You will need this system to evolve with you as new devices are added to your network and upgrades occur.

People have different preferences at this point, but I like to try to narrow the field to two choices before bringing evaluation units onsite. However, I do firmly believe in bringing at least one evaluation unit onsite and installing it into your production environment. The nice thing about SIM solutions, unless you're testing automated remediation, is they shouldn't have any impact on production. Typically, you can change syslog settings and even install agents without having to reboot systems. Make sure the system is everything the vendor says it is. I am very reluctant to do business with vendors who will not either provide a demo unit or provide some kind of, try it for 30 days before you buy it, guarantee.

Once you've made your decision, make sure you've negotiated the best price before passing along the good news. This is a very competitive business; use that to your benefit. If possible, use the tried and true method of buying close to the end of a quarter. The vendor gets a last minute boost to those quarter end numbers and you get the best deal possible.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

As we reach the end of this journey into the world of SIM, hopefully you have a much better understanding of the issues involved in purchasing a SIM and some useful tools to help make the decision process much easier and more effective. SIM is a huge organizational investment and taking the time to get through the lengthy selection process will pay huge dividends in the end. Hopefully you've chosen a SIM solution which can have a very positive impact on your organizations security operations and compliance efforts. Now the real fun will begins; the implementation. Good Luck!

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

7. References

Carr, J (2007, September 1). The sim solution. *Secure Computing Magazine*, Retrieved October 3, 2007, from http://www.scmagazineus.com/The-SIM-solution/article/35618/

McLaughlin, K (2007, February, 5). Be on the Alert: SIM Solutions Take Security Market by Storm. *darkREADING*, Retrieved September 29, 2007, from http://www.darkreading.com/document.asp?doc_id=116373&page_number=1

Nicolett, M & Kavanagh, K. (2007 May 9). Magic Quadrant for Security Information and Event Management, Q107. G00147559, 2. from Gartner.

Rothman, Mike (2007 March 13). Security information management finally arrives, thanks to enhanced features. Retrieved October 11, 2007, from SearchSecurity.com Web site: http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1247084,00.html

Shipley, G (2006, May, 22). Market analysis: security information management. *Network Computing*, Retrieved October 3, 2007, from http://www.networkcomputing.com/showArticle.jhtml?articleID=187203568&queryText=SIM

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Appendix A – SIM Vendor List

Company/Product	Website
ArcSight ESM	www.arcsight.com
CA Security Information Management	www.ca.com
Cisco Systems CS-MARS	www.ciscosystems.com
ExaProtect Security Management System	www.exaprotect.com
High Tower SEM	www.hightower.com
IBM Tivoli	www.ibm.com
Intellitactics Security Manager	www.intellitactics.com
LogLogic	www.loglogic.com
LogRhythm	www.logrhythm.com
netForensics nFX Open Security	www.netforensics.com
NetIQ Security Manager	www.netiq.com
NitroSecurity NitroView ESM	www.nitrosecurity.com
Novell Sentinel	www.novell.com
Open Source Security Information Management	www.ossim.net
Q1Labs Qradar	www.q1labs.com
RSA envision	www.rsa.com
SenSage	www.sensage.com
Symantec Security Information Manager	www.symantec.com
Tenable Network Security's Security Center	www.tenablesecurity.com
TriGeo Security Information Management	www.trigeo.com

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Appendix B – SIM Evaluation Templates

Organizational Requirements

Step 1 Rank, in order from 1 to 4, the reasons for pursuing a SIM solution. **1 being the most important**

Compliance	
Log Aggregation	
Incident Response	
Security Group Efficiency	

Step 2 If compliance is a reason for pursuing a SIM, please list any relevant legislation. (SOX, GLB, HIPAA, etc)

Step 3 Is the organization interested in solutions that are **not** appliance based?

Step 4 Is agent-less log collection a requirement?

Step 5 Is access to logs in raw format a requirement?

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Step 6 How long should logs be kept for?

Step 7 Please rate NBAD (Network Behavior Anomaly Detection) in your SIM search.

Required as part of SIM	
A plus, but not required	
Not interested	
Support for existing product required	
List product if support required	

Step 8 Are automated remediation options a requirement?

Step 9 Do you intend on collecting logs from workstations? If so, list OS and quantity.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

List Log Generating Devices/Applications

Step 10 List antivirus and antispyware software used in the organization.

Manufacturer	Product	Version

Step 11 List authentication sources in the network.

Authentication Source	Version

Step 12 List DHCP Servers used in the network.

DHCP Server	Version

Step 13 List any NAC solutions in place.

Manufacturer	Product	Version

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Step 14 List any management systems already doing centralized log collection.

Manufacturer	Product	Version

Step 15 List the server operating systems in production.

Operating System	Quantity

Step 16 List key applications used in the organization.

Application	Version

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Step 17 List vulnerability scanning/assessment tools used within the organization.

Application	Version

Step 18 List firewalls and intrusion detection/prevention systems used in the organization.

Manufacturer	Product	Version	Quantity

Step 19 List any client-based and/or SSL VPNs used in the organization.

Manufacturer	Product	Version

Step 20 List routers/switches used in the organization.

Manufacturer	Product	Version	Quantity

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Step 21 List wireless access points installed within the organization.

Manufacturer	Product	Version	Quantity

Step 22 List any other network devices not listed above.

Manufacturer	Product	Version	Quantity

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

System Sizing

Step 23 Total number of log generating devices

_____

Step 24 Estimated organizational log volume represented in number of events per second

_____

Step 25 How many days must logs be retained?

_____

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**