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.

Keys to Implementing a Successful Security Information Management Solution (or Centralized Security Monitoring)

Security professionals are inundated with an overwhelming flow of security events from an ever-growing list of assorted security products. Recent trends including government regulations are driving IT to implement appropriate safeguards - one of which is security information management (SIM). SIM provides a way to gather, analyze, and report vast amounts of security information in a humanly understandable way, greatly enhancing the effectiveness of security analysts. While SIM solutions are expensive, they're sorely ne...

Copyright SANS Institute
Author Retains Full Rights

AD

Michael Martin
December 12, 2003
GSEC Practical, Version 1.4b Option 1

Keys to Implementing a Successful Security Information Management Solution (or Centralized Security Monitoring)

© SANS Institute 2004, Author retains full rights.

Table of Contents

Summary 1
Audience 1
The Problem 1
The Solution 2
Keys to implementing a successful SIM solution 5
1. Select the right product 5
Collect requirements 5
Send an RFP to potential vendors 8
Evaluate short-list products in-house 8
Talk to existing customers 9
2. Start with a pilot 9
3. Put your money in storage and database hardware 10
4. Define your environment 11
5. Get good people and train them 11
6. Have a lab system 13
7. Agent and data source integration principles 13
8. Integration and configuration tips 14
9. Measure progress with indicators 15
List of References 16

© SANS Institute 2004, Author retains full rights.

Summary

Security professionals are inundated with an overwhelming flow of security events from an ever-growing list of assorted security products. Recent trends including government regulations are driving IT to implement appropriate safeguards—one of which is security information management (SIM). SIM provides a way to gather, analyze, and report vast amounts of security information in a humanly understandable way, greatly enhancing the effectiveness of security analysts. While SIM solutions are expensive, they're sorely needed to meet today's security challenges.

This paper provides nine keys to implementing a successful SIM solution.

Audience

The target audience for this paper is organizations—government, financial institutions, utility companies, large corporations, and managed security service providers (MSSPs)—with large security budgets and dedicated security operations centers. Budget demands for security software, hardware, supporting security data sources, and personnel easily exceed $1 million.

The Problem

Security professionals are inundated with an overwhelming flow of security events from intrusion detection systems (IDS), authentication systems, firewalls, operating systems, applications, and an ever-growing list of assorted security products. In large organizations with several variants of these systems, this flood of 2 to 50+ million events per day is intimidating.

So why bother with all these events? In the past, financial institutions, the military, and certain government agencies were the primary groups daring enough to analyze this data. However, times have changed. Impetus to monitor security events includes:

- Expanding use of e-business/e-commerce
- Audit and reporting requirements
- Increasing numbers of threats
- Government regulation

In the United States, recent government regulations—such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act of 2002 (Sarbox), and the Patriot Act of 2001—are driving organizations to implement centralized security monitoring solutions. These regulations hold organizations accountable, "meaning IT must implement

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

appropriate safeguards."[1] And according to Network Computing, "about 72 percent of readers polled…say they are affected by HIPAA, Sarbox, GLBA or the Patriot Act."[2]

Problems resulting from maintaining security events from disparate security systems decentralized in individual silos and not having a central security team include[3]:

- Attacks from the same source against different groups are unlikely to be identified as being related.
- Individual system administrators are expected to monitor events and then know what to do in a crisis—instead of one group with in-depth security experience responding to incidents. Administrative duties and system availability typically take priority over security duties.
- Best-known methods for incident handling are less likely to be shared and distributed.

The Solution

To meet these needs, the security operations center (SOC) and security information management (SIM) solutions have recently emerged. An SOC and its outsourced sibling, the MSSP, "centrally manage and monitor their clients' network and perimeter security systems from redundant secure operations centers (SOCs) in real time around the clock."[4] Determining whether to staff your own internal SOC or to entrust an MSSP with your security operations is beyond the scope of this paper. However, both options demand the use of a SIM solution to enable security analysts to meet the demands of their job.

This paper focuses on how to successfully implement SIM, which is also known as security event management (SEM), enterprise security management (ESM), and centralized security event monitoring.

"SIM systems provide a method of gathering, centralizing, managing and presenting [security] data to the user in a digestible manner."[5] To describe it another way, SIM "is a security management and incident response platform designed to improve the effectiveness, efficiency and visibility of security operations and information risk management."[6]

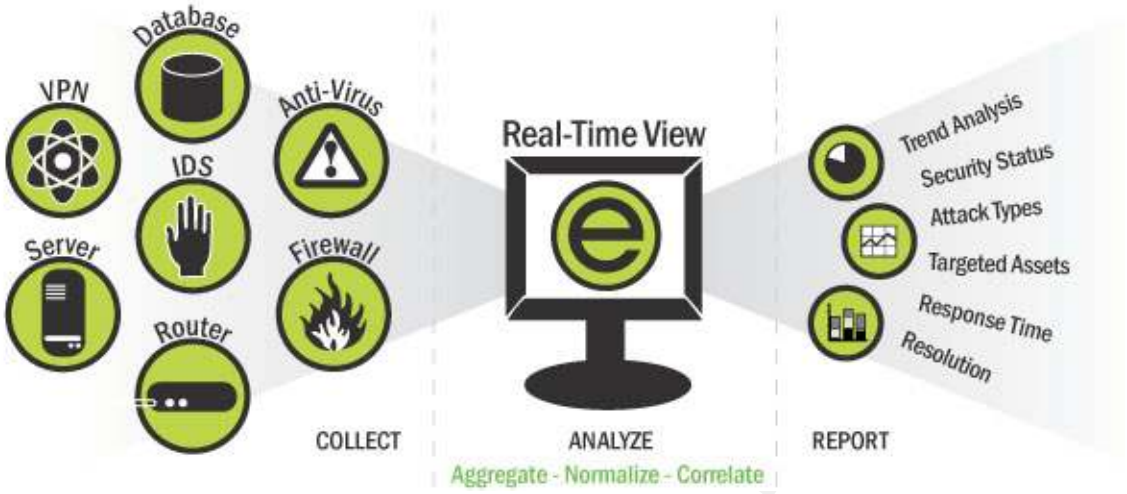
The following figure illustrates the logical flow of SIM.

---

[1] Doherty, 2003
[2] Doherty, 2003
[3] Kohlenberg, 2001
[4] Armstrong, 2003
[5] Shipley, 2003
[6] neuSECURE, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Figure 1[7]



According to Richard Stiennon of the Gartner Group, "Security event management solves today's critical problem of aggregating and correlating diverse log data for real-time event detection and response. In the future I see these security management platforms serving as the central intelligence systems for security operations."[8] Well, the future is here.

In a review of SIM products in the September-October 2003 edition of *Secure Enterprise*, the writers concluded "Although SIM suites are pricey, the products are evolving rapidly, and *we can't imagine running a modern-day SOC without the functionality they provide*"[9] (emphasis added). If you looked at these solutions a year or two ago and weren't impressed, it's time to look again.

A SIM solution typically consists of the following components:

- **Correlation Engine** – associates seemingly meaningless individual events with security events from other data sources to identify incidents requiring an analyst's attention.
- **Database** – provides persistent event storage for forensics.
- **Agents** – collect security events from virtually any security data source, normalize the events into a standard format, and send the events to the correlation engine in a secure channel.

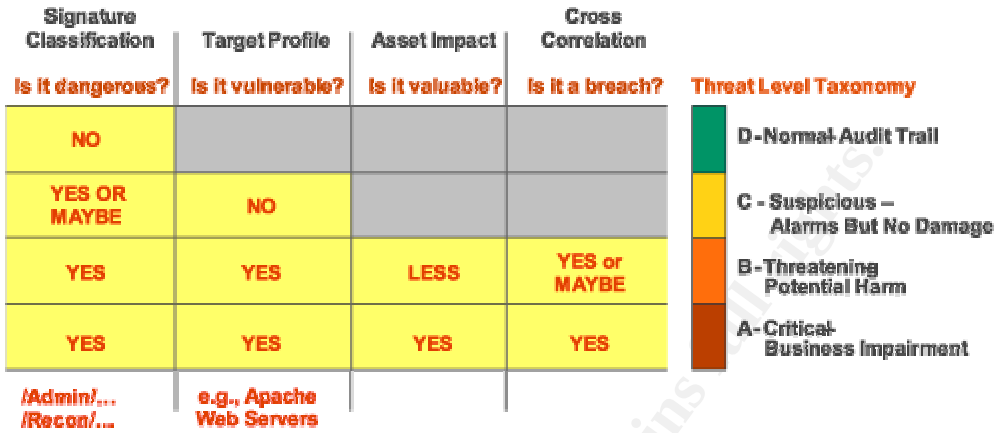
Due to sheer event volumes, the value of correlation cannot be overstated in helping security analysts detect and respond to the highest priority matters quickly and efficiently. The following chart illustrates the analysis performed by

[7] e-Security, 2003
[8] neuSECURE, 2003
[9] Shipley, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the correlation engine that priorities each event beyond the original alert severity determined by the system that generated the event.

Figure 3[10]



ArcSight Security Intelligence Taxonomy

Excellent sources that further explain the value of SIM, describe its components, and provide a partial list of vendors include the recent *Secure Enterprise* article[11] and Patrick Nolan's paper[12].

As mentioned, SIM solutions are pricey and start around $250,000 for a medium-sized implementation (see pricing below for a small installation). Pricing is usually based on the number of devices reporting into the system.

Figure 2[13]

SIM Pricing	ArcSight 2.2	eSecurity 4	GuardedNet netSecure 1.6.1	Intellitactics Network Security Manager 4.0	netIntensics 3.1	Network Intelligence Engine - A Series 1106
Price as tested in our environment (no hardware), less than 25 devices	$67,500	$115,000	$70,000	$100,000	$60,000	$28,000*
Price for 100-device support (no hardware) and 4 admin consoles	$162,500	$260,000	$144,000	$110,000	$150,000	$61,000*

*Approximate includes hardware and software

[10] ArcSight, 2003
[11] Shipley, 2003
[12] Nolan, 2003
[13] Shipley, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Keys to implementing a successful SIM solution

Before making the investment in SIM, please consider the following steps to guide you to a successful implementation.

1. Select the right product

Choosing the right product is vital to your organization's success in managing security event data. While the steps suggested below may sound tedious, they will ensure you're on your way to making a good decision.

Collect requirements

Gather customer requirements and document them in a customer requirements document. Although time consuming, you'll find it worthwhile since you'll need the requirements later for the RFP and the test plan used for your in-house evaluation.

While this is not a comprehensive list, consider the following features to select the right product for your environment.

Feature	Benefit
Integrate with current security and application solutions in the environment[14] • Currently supported security products • Agent SDK	Handles all security solutions in your environment • Host IDS, network IDS, firewalls, routers, honeypots, authentication systems, trouble-ticketing systems • Enable integration with third-party products and custom applications through a variety of integration methods (log files, ODBC, sockets, serial ports, OPSEC, Cisco SDK, SNMP, etc.[15])
Asset information – Import information about network devices, servers, client PCs, etc. so they can be categorized by criticality, location, business group, etc.	Enhances correlation capabilities so that all IP addresses are *not* alike.
Event categorization – Events from different vendor's products are categorized into similar classes (recon, attacks, etc.)	Correlation rules can be written based on general categories (e.g., recon followed by exploit attempt), so when a security data source is added or removed from the environment, you don't need to rewrite all the correlation rules since they're not product specific.

[14] Patel, 2003
[15] e-Security, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Feature	Benefit
Easy-to-write correlation rules	Simplifies the skill set required by security analysts since they don't need programming knowledge.
Correlate events into incidents ("an incident is a set of related security events"[16])	"Reduces the amount of data an analyst must examine in order to identify and assess threat activity."[17]
Secure communications – End-to-end network transport of all security events are secure	Encrypted communications ensures confidentiality of security events originating from authenticated data sources (integrity).
Intuitive user interface • Display correlated events, which are collections of related events • Drill down to packet-level event details • Customizable at-a-glance security views for each analyst • Simultaneous access to real-time and historical events • Integrate with third-party knowledgebases	• Reduces the security event overload for security analysts. • Saves time so analysts don't need to use other security product consoles. • Saves analyst time by allowing them to save views for their specific needs. Detect sensors down, surges in specific protocols (e.g., UDP). • Facilitates forensics to see real-time events (e.g., activity from one source IP) in a historical context. • Saves analysts time when they can reference a security product's knowledgebase directly from an event.
Database • Robust performance • Database management utility • Event aggregation "A process of de-duplication that reduces large volumes of event data into a manageable set."[18]	• Enables responsive queries with millions of events in persistent storage. • Reduces database knowledge required by engineers for partitioning data by day, week, etc. and pruning data to be stored offline. • Reduces the amount of storage required. "This is especially useful for events such as ping sweeps or port scans where similar events are reported multiple times by firewall devices."[18]
Agent • Supported operating systems – Make sure the agent runs on the operating systems you plan to use in your environment.	
Scalable architecture – Enable deployment of multiple correlation engines and databases in a hierarchical configuration to accommodate growth	Offers a solution architecture you can grow with.

[16] Geijn, 2003
[17] Geijn, 2003
[18] netForensics, Aggregation, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Feature	Benefit
Vulnerability assessment integration	Enables threat analysis and enhances correlation capabilities by determining if a target is vulnerable to the attack launched against it.
Notification – Provide standard notification methods (email, pager, etc.) for both security and system events	• Engineers can be notified of significant events (e.g., low disk space, agent down, etc.) when not in front of the console. • Security analysts can be notified of significant security incidents when not looking at the console.
Case management – Offer strong case management capabilities or tight integration with an external issue tracking system	Analysts can record progress on incidents, transfer knowledge to other analysts during shift changes. In addition, managers can track operational metrics such as cases created from incidents, average closure time, etc.
Reporting • Useful standard reports • Powerful custom report authoring capabilities • Scheduled report capabilities for automated report generation	• Reduces workload and provides examples for other reports you may need to create. • Create the reports that your management really wants. • Reduce workload to generate periodic reports.
Administration • Track system component availability • Granular access control • Agent software distribution	• Early warning of issues with correlation engine, database, agents, or sensors. • Assign privileges as needed, but not more permissions than necessary. • Reduce administrative workload through automated deployment of agent updates.
Visualization Graphical representation of events	Enables quick understanding of related events (e.g, identify DDoS targets). While strong opinions exist on this topic, this is more of a "nice-to-have" feature than a mandatory "bread and butter" feature.
Company background General characteristics for a company that you will rely on: • Responsiveness to your needs – How responsive are they to your feedback (feature requests, product defects, etc.)? For example, ask for custom database indexes. • Financial stability – Will they be around in 2-3 years? (Many companies in this evolving market segment are small. If you're concerned about their long-term viability, ask to place their source code in escrow.) • Technical support – these products are relatively complex, and all products have defects. Test out their technical support before you buy. • Training – find out if they offer an official curriculum that covers more than just the basics. You'll need to know this product thoroughly to be successful. • Experience with large environments	

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Send an RFP to potential vendors

Compile your requirements into an RFP and send it to potential vendors. Then rank the RFP responses. If you have more than four vendors on your short list, request web meetings with each vendor to demonstrate key product features. This will help to clarify their RFP responses.

When making your "short list" of vendors, quickly eliminate products that:

- Can't scale (e.g., use an Access/Jet database that can't handle high event loads, concurrent users, etc.)
- Lack third-party product integration (e.g., support products primarily from one vendor and perhaps a popular firewall)
- Lack solid correlation abilities (e.g., provide basic correlation for only a few fields)
- Don't meet your basic requirements and the vendor is pitching the roadmap (no tangible product)
- Require inordinate amounts of hardware.

Evaluate short-list products in-house

After the RFP and web demonstrations, take the time to test the products on your short list in-house to determine their true capabilities. Hands-on, in-house testing against your documented requirements is essential to ensure the product's abilities match the vendor's claims and meet your needs.

Secure Enterprise recommends the following critical questions[19]:

> **Critical Questions**
> Here are five critical questions every organization should have a handle on before going into a SIM testing or pilot program.
>
> **1. Know how you will handle logging and data-transport issues.** Do you need to support alerts in formats other than syslog? Do you want to aggregate insecure transport mechanisms, such as syslog or SNMP, to local aggregation points and retransmit using secure agents, or will you send data in the clear? How many alert protocols will you have to support?
>
> **2. Have estimates on data loads, both eps (event per second) levels and size (for example, gigabytes per day or week).** Without knowing the level of alerting your devices will produce, it's difficult to successfully plan and deploy a SIM system. You also run the risk of saturating your bandwidth-challenged WAN connections.

[19] Shipley, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. Know what retention range you're shooting for. Regulated industries may be required to save logs for a prescribed amount of time. Even if your organization is not regulated, having a data-retention policy—and sticking to it—is a good practice.

4. Once you know how much data you're going to have and how long you need to keep it, start planning where data will be stored. If you need to budget for a SAN to hold six months of logs, better to figure that out now.

5. Know the limitation of your SIM device when it comes to data administration. Many security teams lack a full-time database administrator, and some of these products require heavy relational-database knowledge to manage data. If you're going to need database-admin skills on an ongoing basis, factor those costs into the plan up front.

To adequately test the product, connect it to several *high*-volume data sources such as firewalls, *untuned* network IDS sensors, and a custom or not-yet supported data source if possible. This will enable you to validate the product's correlation abilities, scalability, and performance. In addition, you'll see how long the vendor takes to integrate a product that they don't currently support. During the evaluation, contact their technical support a few times to see how available, knowledgeable, and useful they are.

Talk to existing customers

When you've decided on a product, ask for two to three customer references. Then either call or visit them. For security products, visiting isn't often an option, but it's worth asking. Occasionally vendors have reference accounts that use their product for little more than shelfware. Find out their perception of the product, how they use it, how widely deployed it is, issues they've encountered, the vendor's response to those issues, their experience with technical support, successes, etc.

2. Start with a pilot

Once you've purchased a SIM product, start with SIM training. Then begin your deployment with a pilot instead of trying to conquer the world in a day. Chances are good you'll gain several key learnings and develop important processes in the pilot that will help in further deployments. With the experience level of your security analysts as the primary gating factor, you can integrate more data sources at your desired pace.

Depending on the experience of your security analysts and the pace at which you collect and import network/system information in the SIM system, plan on about 3-6 months to begin feeling like you've got a grip on high-powered security event monitoring.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

3. Put your money in storage and database hardware

In a SIM system, the biggest bottlenecks are the database and storage. Allocate generously to these components (don't skimp!) or performance will suffer dramatically. Ever increasing security event numbers caused by integrating additional security data sources, worm outbreaks, etc. result in ever-expanding storage needs.

A high-performance SAN is the best option if you don't want a cap on your storage capacity. Aside from "Critical Questions" 3 and 4 in Key #1, factors to consider for a SAN include:

- Number of drives
- Drive speed (10K rpm, 15K rpm, 25K rpm, etc.)
- RAID level – some database vendors recommend RAID-10, but RAID-5 may work as well or almost as well if cost is an issue.
- Controller cache size
- If you're using Logical Units (LUNs) and sharing the physical drives with other applications, what performance impact do the other applications impose?

For your database, typical bottlenecks are I/O and memory. Consider the following in your purchasing and configuration:

- Buy as much memory as possible for your database server—and make sure the OS can address the memory. The database server should have at least 4 GB of RAM.
- Configure the database to *use* the memory. The vendor's embedded database install will not likely maximize the memory usage to its fullest capacity.
- Assign the most I/O-intensive parts of the database (data, indexes, transaction logs, etc.) to separate SAN LUNs to reduce spindle contention.
- If applicable to your database and OS, ensure that the cluster/allocation unit size are the same on the file system, controller, and database to optimize performance.
- Processor utilization is not typically a database bottleneck. Average database processor utilization is likely between 5-20%.
- Buy a 1Gb network adapter

While your hardware requirements will vary depending on the product you use, the following guidelines are useful:

- Correlation engine server
  - Processor – depending on your hardware platform, a hyper-threaded dual-processor server is probably more than enough.
  - RAM – some correlation engines don't take advantage of more than 1 GB of RAM for the correlation engine itself, so 2 GB of RAM for the server is plenty.
  - Mirrored hard disk drives

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

    - Network interface – 1 Gb network adapter since the highest sustained rates are usually between the correlation engine and the database.
- Agent server
    - Processor – dual-processor server
    - RAM – 1 GB of RAM
    - Mirrored hard disk drives
    - Network interface – a 1 Gb network adapter is probably overkill, but it depends on the event flows from the particular data source.

4. Define your environment

Let the SIM product know your environment as much as possible by importing the following:

- Networks – internal, VPN, dial up, DMZ, wireless, etc.
- Asset information – this can be automated with either vulnerability assessment or asset management tools. You can import fields such as:
    - Criticality (Critical, High, Medium, Low)
    - Operating System
    - Applications
    - Vulnerabilities – providing the correlation engine this information further reduces noise and highlights significant issues for analysts. Some question the accuracy of correlating IDS alerts and vulnerability assessment results via BugTraq IDs (BIDs), but can you afford manual human association instead of automatic correlation?

The more information you import into the system, the greater the dividend you'll receive in effective correlation and noise reduction.

5. Get good people and train them

To run a typical SIM solution, you'll want two engineers to provide adequate coverage for vacation, sickness, training, etc. Although this paper doesn't cover SOC analysts specifically, they are mentioned since they are involved in ongoing operational aspects of a SIM system. A suggested division of labor with backgrounds and training follows:

SIM Engineers

- Background
    - Security training with a background in operating systems (Windows, Linux, and UNIX variants), databases, networking, and engineering
- Recommended Training
    - Security training covering general security like GSEC
    - SIM product training
    - Database training

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

        - The engineers need to be comfortable with the SIM database. They should at least take an introductory class so they're comfortable executing SQL commands at a command prompt if asked by the vendor and using the database GUI (e.g., Oracle® Enterprise Manager or Microsoft® SQL Server™ Enterprise Manager)
        - "Most customers report that a part-time DBA is more than sufficient to manage [an] … installation…. dedicating only about 25% of one DBA…."[20]
    - Product training on each integrated security product (e.g., HIDS, NIDS, firewall)
- SIM Duties
    - Install and configure SIM product
    - Manage SIM database
    - Integrate new data sources (test standard agents, configure custom agents)
    - Testing OS and SIM patches, as well as new versions

Second-Level Security Analysts

- Background
    - Security training and certification with a background in operating systems (Windows, Linux, UNIX variants, mainframes, etc.), networking, and operations
- Recommended Training
    - Security training such as GCIA, GCIH, GCUX, etc.
    - SIM product training focusing on the features they use (console, writing correlation rules, etc.)
    - Product training on each integrated security product
- SIM Duties (other security duties are not listed here)
    - Create and maintain:
        - Correlation rules
        - Views/filters – create default views to determine what first-level analysts see
        - Assets/groups/zones
        - Lists (e.g., suspected/untrusted IP addresses)
        - Reports

Recruiting

While technical skills are important, they can be learned. Personality traits are sometimes harder to change, so here are a few suggestions for security analysts:

- Highly ethical (since analysts are exposed to highly sensitive data)
- Highly motivated to work in security
- Able to handle information overload
- Aptitude for continuous learning

[20] netForensics, Embedded Database & Utilities, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

6. Have a lab system

When purchasing hardware for your SIM system, make sure that you've budgeted for a full lab environment to test in. Integrate new data sources into the lab first. Once you've characterized the event loads to ensure proper tuning has taken place, DNS entries exist, etc., migrate the new data source to your production system.

The same holds true for OS and vendor patches, as well as new releases. Regardless of the QA performed by the vendor, there is usually a need for support pack 1 (and 2, etc.). In addition, New security analysts quickly become gun-shy writing correlation rules if they write a new correlation rule with a circular reference on a production system that brings the system to its knees. A good lab system resolves these issues.

7. Agent and data source integration principles

- **Aggregate/consolidate data as close to the source as possible.** Minimize SIM agents by placing them on the aggregation points (databases) themselves. This also eliminates insecure ODBC connections to retrieve the events.
  - Point Product Databases – Many host IDS (HIDS) solutions and network authentication systems have centralized databases. For HIDS, this is the management database that stores HIDS events and agent configurations (e.g., Symantec Intruder Alert™, ISS ICEcap®/SiteProtector™, Sygate Secure Enterprise, Zone Labs Integrity™). For network authentication (VPN, dialup, etc.), this is the RADIUS database.
    - Install the SIM agent on HIDS or RADIUS database, if politics allow. Agent resource loads are usually minimal and should not impact the server's primary application.
  - Custom Protocols – Many appliances like firewalls (Cisco® PIX®, Check Point™ FireWall-1®, etc.) and some network IDS (NIDS) sensors (Cisco Secure IDS, Sourcefire Management Console, etc.) have custom protocols like OPSEC and Post Office Protocol or APIs.
    - In these cases, the SIM vendor develops an agent that communicates using the same protocol. This agent runs on a dedicated server located as close on the network as possible to the data source. Depending on the protocol, it may range from authenticated and encrypted to unauthenticated and unencrypted. Understand the protocol and its inherent risks.
  - Intermediate Databases – For some network IDS products like Snort™ and Symantec ManHunt™, you may need to configure an intermediate database to store "trigger" packet-level data so that it's available to the SIM solution. Otherwise you'll get just the alert

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

without the payload, making it difficult to establish an event's validity. Many of these can be NIDS can send events to either MySQL™ or Oracle®. A single database server can consolidate events for several NIDS sensors.
    - Install the SIM agent on intermediate database server.
  - Syslog – For logs from routers, proxy servers, DNS servers, or other application servers, consider aggregating the data on a syslog server.
    - Install the SIM agent on syslog server. This is a good configuration for systems in your DMZ, so syslog traffic is kept local, logs are stored on a secure syslog server, and events are sent by the SIM agent on a single encrypted TCP port through the firewall.
- **More data is good—as long as it's good data.**
  - Surprisingly more data—if it's good data—can improve correlation and reduce security analyst work loads instead of increasing them. Refer to the network authentication integration tip below to see how including VPN data automates dynamic host name and IP address resolution, greatly reducing manual research by analysts to see who leased an IP address for a specific time period.
  - The axiom "garbage in, garbage out" holds true with SIM, and the system is only as good as the data feeding it.
  - "Monitoring IDS, firewall, authentication, system and application events has become critical to successful security."[21]

8. Integration and configuration tips

Vendor documentation is generally good at stating how to do basics, but several lessons are learned through hard knocks. Here are a few tips that will hopefully help you avoid some pitfalls and assist in a faster, more successful deployment.

- **Integrate network authentication systems early.** Network authentication systems like VPN and dialup systems provide immediate value in SIM systems. SIM consoles typically show source IP address and target IP addresses as part of an event. How do you identify the person associated with the IP address? What if your environment is predominantly DHCP or has a high percentage of telecommuters or wireless LAN users authenticating through VPNs? VPN and dialup gateways usually assign dynamic hostnames and IP addresses to users who may be connected for 5 minutes or 12 hours. Integrating the RADIUS data for VPN and dialup will populate your incidents with the user IDs assigned to the dynamic IP addresses for that moment in time.
- **Require time synchronization.** If business groups want to integrate their existing network IDS sensors (or other data sources), respond "Great! We'll integrate your systems once time synchronization is enabled."

[21] Shipley, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Without time synchronization, system clocks easily drift by as many as 60 minutes. In addition, some users purposely set their clocks ahead by several years, which makes correlation more difficult. Many earlier commercial NIDS products do not natively support time synchronization (e.g., ntp).

- **Learn how to filter out bad signatures at the agent level.** In some scenarios, the SIM engineering team won't own any of the data sources feeding into it. If someone on a different team enables a bad NIDS signature that fires on every DNS query and then the person leaves on vacation, you'll experience a lot of false positives that can quickly fill your database with garbage. For these scenarios, learn how to filter specific events at the SIM agent so they won't reach the correlation engine and database.
- **Agent threads – default settings aren't always the best settings.** Similar to the database memory settings discussed earlier, agents may come configured with a single thread to communicate with the correlation engine. For low-volume data sources this works fine. However, if a few chatty NIDS sensors are forwarding events to an agent, the agent may need to forward an average of 250+ events per second. With only one thread enabled, the agent will immediately begin caching events since its communication channel is saturated. Find out how to configure your agent's threads, event batching, time correction, etc.
- **Establish a business continuity plan (BCP).** What happens to your SIM system when the power grid goes out like the August 2003 episode in the northeastern United States[22]? Assuming your UPS has a lot of fuel, you're probably okay. For SIM project managers with less-than-ideal budgets, here's a high-availability BCP alternative to clustered servers that may make sense. Establish two sites—perhaps on opposite sides of the country or globe—each with a non-clustered correlation engine and database. Then configure each SIM agent to forward events to both correlation engines. If one site drops off the map, security analysts can simply point their consoles to the other site without a loss of data.

9. Measure progress with indicators

Indicators are vital to ensure the success and longevity of your SIM project. Otherwise, management won't see any visible return on its security investment. While far from complete, here are a few security indicator ideas to get you started:

- Issue containment times (malware, virus outbreak, intrusion, etc.)
- Value of security – internal incidents versus external industry averages
- Blocked intrusions – if you have intrusion prevention systems (IPS)
- Enforcement actions taken – enforcement resulting from SIM information such as removal of compromised systems, investigations, etc.

[22] CNN, 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

List of References

ArcSight. "Product Information." URL: http://www.arcsight.com/product_info01.htm (12 December 2003).

Armstrong, Illena. "Your safety in a stranger's hands: Getting bang for your buck." SC Magazine. September 2003, URL: http://www.scmagazine.com/scmagazine/2003_09/feature_2 (11 December 2003).

CNN. "Major power outage hits New York, other large cities." URL: http://www.cnn.com/2003/US/08/14/power.outage/ (12 December 2003).

Doherty, Sean. "Feds Reach Out and Touch IT." Network Computing. 10 July 2003. URL: http://www.nwc.com/1413/1413f1.html (9 December 2003).

e-Security. "Agent Technology." URL: http://www.esecurityinc.com/products/agent_technology.asp (12 December 2003).

Geijn, Ronald Van and Craig Robinson. "Know your terminology." SC Magazine. September 2003, URL: http://www.scmagazine.com/scmagazine/2003_09/cover/ (11 December 2003).

GuardedNet. "netSECURE Overview." URL: http://www.guardednet.com/prod.html (12 December 2003).

Kohlenberg, Toby. 2001. Unpublished paper used with permission.

netForensics. "Aggregation." URL: http://www.netforensics.com/documents/pr_sim_sublinks.asp?id=2 (12 December 2003).

netForensics. "Embedded Database & Utilities." URL: http://www.netforensics.com/documents/pr_embedded.asp (12 December 2003).

Nolan, Patrick J. Jr. "Security Information Management." 1 September 2003. URL: http://www.giac.org/practical/GSEC/Pat_Nolan_GSEC.pdf (9 December 2003).

Patel, Upesh. "Five additional questions to ask about a SIM solution." SC Magazine. September 2003, URL: http://www.scmagazine.com/scmagazine/2003_09/cover/ (11 December 2003).

Shipley, Greg, Tom Oele, with Mike Janowski. "Too Much Information." Secure Enterprise.12 September 2003, URL: http://nwc.securitypipeline.com/trends/showArticle.jhtml?articleId=14700464 (9 December 2003).

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 22nd, 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**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**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**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 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**