



From Logs to Logic: Best Practices for Security Information Management

by Gretchen Hellman

As cyber-criminals get smarter and smarter, staying one step ahead of emerging security threats is getting harder and harder. Seemingly every day, news reports are filled with hair-raising stories about computer networks and corporations being terrorized by worms, viruses, hackers and identity thieves. More than ever, companies need to pay strict attention to network security, not only to defend against attacks and protect customer data, but also to satisfy a growing list of government regulations like Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), California's privacy breach notification law SB1386, and the Federal Information Security Management Act (FISMA).

Organizations large and small have attempted to protect themselves by pouring millions of dollars into technology-enabled security solutions like antivirus gateways, firewalls and intrusion detection systems. But this has led to a new problem: crippling complexity. As a result, companies are now burdened with trying to manage dozens - sometimes even thousands - of security devices and systems from many different vendors. This number of disparate devices generates a deluge of data, often billions of events per day, primarily consisting of false alarms. These false alarms can overwhelm security operations and waste valuable time and money by leading security analysts on a fruitless hunt for random events.

With so many event logs generated each day, identifying perimeter security, insider threat and compliance issues within this sea of information can be an impossible task. This article takes readers through best practices for turning technical data points into business-relevant information including:

- What technologies are available to help with this problem?
- What data sources will yield security relevant information?
- How to institute an effective monitoring and review program.
- How to make a log review program apply to policy.
- What are the best practices for conjoining security information with business risk?

Part A: Introducing the Problem

Drowning in Data

Security Information Management (SIM) is the centerpiece of any strong security management program. With the growing number of worms, viruses, hackers and malicious insiders-combined with the new millennium's exploding regulatory environment-organizations are adopting best-of-breed security infrastructures to protect themselves. But by pouring millions of dollars into a wide array of security solutions like antivirus gateways, firewalls and intrusion detection systems, organizations have exposed themselves to a quagmire of complexity.

Without intelligent centralized management, many enterprises have found that their security programs have evolved into a complex patchwork of disparate systems that generate an overwhelming flood of data but offer little visibility into true threats and attacks. While this was acceptable in the past, cost concerns, coupled with increasing regulatory compliance pressures and an ever-evolving threat landscape have seen more and more companies shift to adopting SIM technology to centrally manage information risk and protect critical IT assets.

Meanwhile, government regulations like SOX, HIPAA, SB1386, and FISMA have raised the stakes when it comes to protecting sensitive data and processes, including the integrity of the financial reporting process and the protection of personally identifiable information (PII). Businesses are often compelled to report weaknesses in financial controls,

database breaches and information loss. Failure to protect sensitive data and meet regulatory requirements can destroy customer trust, lead to cancelled contracts, spur government and industry fines, damage stock prices and invite class-action lawsuits. More than ever, organizations need automated, auditable and focused log consolidation and review to meet government IT related regulations.

In addition to the compliance problem, the prevalence and damage caused by attacks have grown to staggering proportions. These attacks are not only increasing in frequency, but in complexity and severity as well. The time-to-exploitation of today's most sophisticated worms and viruses has shrunk from years to months to days, and in some cases, to a matter of hours. Defending against these attacks is becoming more difficult by the minute.

It is not just external attacks that organizations must defend against, but malicious insiders who aim to steal confidential customer and business data and sell it for financial gain. Some 35% of the top 100 financial institutions were victims of insider attacks in 2004, compared to only 14% the year before, according to new study from Deloitte & Touche.

Part B: Solving the Problem

SIM to the Rescue

This is where Security Information Management (SIM) technology enters the picture. SIM solutions enable organizations to manage information risk and protect critical IT assets by automatically collecting, correlating and analyzing all security data within a single, intelligent system. SIM allows security teams to manage regulatory compliance requirements, communicate the status of security to a broader audience and gain visibility into insider threats, all while ensuring protection at the perimeter.

When researching the SIM market, however, security professionals may find it difficult to wade through vendor marketing messages and pinpoint significant differentiation. This should come as no surprise, especially as there are no standard definitions for popular SIM-related terms such as "events per second," "correlation" and "asset criticality." This allows some vendors to boast performance numbers, analytics, features and benefits that may be inaccurate or misleading. As a result, organizations are finding that their SIM implementation may not achieve the value originally promised if they have not performed a thorough proof of concept.

The SIM market has grown significantly over the past years and the technology has rapidly advanced. Beyond basic company viability, look for a vendor that has a technology built specifically for the enterprise SIM market, has a proven track record with partners and can address your changing business needs.

The First Step: Define Operational Requirements

It can be difficult for organizations to have a clear vision of what they need to do with their event logs, because they are still so overwhelmed by data overload. The first step in transforming the data overload problem into a SIM based solution is to define operational requirements.

The value of any SIM product is directly related to the data that is input into the system, what meaning the system can derive from the data, and the actions the system is programmed to take as a result of the data. Checklists can be useful, but they must be tailored to reflect the operational requirements of the organization. To effectively refine checklists, you must first determine the primary use cases for the product. Common use cases include:

- **Support for 24x7 security operations center.** Features that are critical to evaluate for this scenario are workflow, customization capability, prioritization, knowledgebase capabilities, correlation intelligence and accuracy.
- **Using the SIM as a "virtual SOC."** This option is for organizations whose budgets do not allow for the implementation of a 24x7 security operations center or organizations that have a higher risk profile. Features and capabilities that are critical for this purpose are correlation intelligence, the ability to tune alerts and rules to eliminate false positives and an equal emphasis on real time and historical analysis.
- **Audit and compliance capabilities.** Audit and compliance requires the integration of a largely different set of data sources, such as operating systems, mainframes, databases and identity management applications. Ensure that your vendor offers the ability to build customized agents for devices that are not immediately supported. While some SIM products offer templates for reporting, it is even more critical for the product to offer significant customization and process support capabilities to draw out information relevant to the defined compliance program.
- **Insider threat.** This use case requires internal devices to monitor trusted user activity and identify suspicious or unauthorized use of confidential information. Even more than audit and compliance, this

scenario demands comprehensive analytics, a robust data set and the integration of non-traditional data sources. Key SIM requirements are the proven ability to integrate with applications, databases, operating systems, identity management and physical security systems that assist in profiling trusted user activity, the flexibility to baseline and analyze based on behavior and the inclusion of specific profiles for time of operations.

Part C: Yielding Security-Relevant Information

Not All SIMs Are Created Equal

Once operational requirements have been defined, the next step is to ensure that the SIM solution can support what will be needed today-and tomorrow. Keep in mind that not all SIM solutions are equal, and that they accomplish tasks with varying degrees of accuracy, flexibility and automation.

For instance, SIM solutions must be flexible enough to handle a wide range of security and non-security devices, such as firewalls, intrusion detection systems, operating systems, applications, network infrastructure, identity and access management systems, databases, and anti-virus solutions that together can yield billions of events per day in an enterprise environment. In this case, a SIM solution must have the ability to review event logs from different devices in different ways. For example:

- Intrusion detection system log review first requires the elimination of false positives, a manual and time consuming task that requires correlation with other devices to determine root cause.
- Database, application and operating system logs must be reviewed to monitor administrative activity and validate that data access rights are appropriately given and appropriate used. This review is part of a strong IT governance program and is required directly by regulatory compliance requirements and/or audit results, depending on the regulation.
- Network infrastructure and firewall logs yield important information about organizational security posture and, appropriately dealt with, can be used to identify zero-day attacks, lax change control and other issues. But leveraging the data manually can require hours of effort for only a small fraction of the information that is generated on a daily basis.

100% Data Collection

The ability to capture and normalize all relevant information is essential for a SIM solution to deliver true value. Systems that can collect and normalize 100% of event data ensure that rich, process-ready information is available for real-time and historical analysis.

A little known fact, however, is that some SIM solutions do not prepare all the data for processing. Make sure that your SIM solution can capture and normalize all relevant information, not just the most commonly used data, such as source IP, destination IP and time and event description. A superior SIM solution will also be able to normalize all event data, rather than simply truncating event data or wrapping into a string that cannot be used efficiently in correlation. This ability to normalize data will greatly enhance real-time threat management and investigation capabilities.

Data Integration: A Key Piece of the SIM Puzzle

The ability to get data into the system is critical to the success of any SIM implementation. SIM users typically face two serious challenges:

- The need to integrate data that is not supported by the SIM vendor.
- Lag time between a new release of a third-party product and SIM support for that new product.

Be wary of vendors that support only a limited number of products or that list a number supported products as under development. This is a sure sign the vendor does not have an agile agent support process. Ask vendors for information about their agent development process, strength of partnerships with supported product vendors and number of supported products. Also evaluate the vendor's custom agent development capabilities. Ask about custom agents that are being used at customer sites, the number of customers that are currently developing their own agents with the provided toolkit. In addition, validate that traditional agent features are available for custom developed agents. Some vendors only offer simple parsers under the guise of a complete agent development environment. This simplification has been known to severely degrade custom developed agent performance.

Part D: Instituting an Effective Monitoring and Review Program

Know the Meaning of Correlation

Correlation is critical because it allows for accurate and automated prioritization and identification of true threats and compliance issues in a business relevant context. But, like many SIM terms, the word correlation lacks a standard definition. SIM technologies that claim to perform asset, vulnerability and event correlation achieve this with varying methodologies and degrees of success. Issues to research include:

- How does the product perform cross-device correlation? Cross-device correlation is key to deriving true analytic value from a SIM solution. Products that do not offer a central categorization language mapping device events to a common taxonomy cannot be used in extensive cross-device categorization. By contrast, products with a categorization language can automatically input language for each device type, leading to greater efficiency and less complex correlation rules.
- How does the product derive priorities? All SIM products derive priorities differently. Make sure prioritization can be determined by the severity of the attack, the criticality of the asset and the vulnerability status of the target relative to the specified attack. It is also important to determine if priorities are adjustable. After implementing a SIM, organizations will need to tune prioritizations based on unique factors such as known false positives and high-risk attacks as well as define customized priorities based on correlated rules.
- How does the product process vulnerability information? Most SIM vendors claim to support vulnerability data, but the breadth, depth and applicability of integration can vary. Key aspects in determining the value of integration include:
 - Automated population of assets with discovered vulnerabilities.
 - Support for a wide array of vulnerability assessment tools
 - Active use of vulnerability assessment information in reducing false positives, prioritizing incidents and correlation functions.
- How does the product incorporate asset value? Incorporation of asset value is performed with varying degrees of extensibility. Determine how the vendor populates and leverages business and technical asset categories in its correlation and prioritization capabilities. Extensibility is also key to melding the product's analytics to your organization. Ask your vendor to create a custom asset category and associate risk-relevant actions for attacks against that asset.
- How does the product track and escalate threat levels? With billions of events per day, the ability of a SIM to track activity and escalate based on successive attacks is critical to identifying and responding to the most dangerous threats. Evaluate how the product uses prior activity in the correlation equation to identify truly threatening or sophisticated malicious activity.
- What are the product's anomaly detection capabilities? Anomaly detection is important to recognize bursts or increases in activity that could indicate a threat.
- What types of statistics does the product produce? Depending on the vendor, statistical correlation can mean anything from simple event counts to statistically derived priority scores. Validate the statistical correlation capabilities of your SIM product to determine the data value your organization will derive from statistical correlation capabilities.
- Can the product correlate new rules from real-time and stored data? It is important to correlate both in real-time for incident response, and also analyze historical data with newly derived correlation rules to address forensics requirements.
- Can the product automatically discover unknown threats? While correlation rules can find known threats, potential SIM customers should inquire about additional analytics that identify unknown threats and bring this knowledge back into the SIM system for future identification.
- How does the product deal with time in the correlation process? The accuracy of a SIM product is often directly related to how the solution deals with time. Some SIM solutions only correlate based on the time-stamp of receipt on the central correlation engine. This limits the system's ability to perform accurate and effective correlation. In addition, it is important to recognize insider activity if it is at an uncommon or suspicious time of usage. If your organization has an interest in insider threat detection or robust audit capabilities, validate that your vendor provides the ability to identify suspicious usage based on time of operations.
- How valuable are default correlation rules? The effectiveness of a SIM product's correlation capabilities can most often be detected by the value of the default correlation rules. Find out what default correlation rules are providing the most benefit to each vendor's customers and how.
- How easy is it to alter, tune and author new rules? Enterprise security teams will derive a long lifetime of value out of a SIM product if the interface allows for intuitive, customized tuning and authoring of correlation rules. Conversely, the lack of a robust authoring system will lead to significant roadblocks. Provide both a simple and complex use case to each vendor and ask them to demonstrate rule creation.

Gain Situational Awareness

When seconds mean the difference between a successful or thwarted attack, gaining situational awareness is critical. After a security incident, the ability to quickly perform forensics allows the organization to prevent a similar attack from recurring. SIMs play a tremendously important role by shrinking the window of vulnerability and allowing organizations to continuously maintain a state of situational awareness via real-time consolidated, risk-relevant views.

Some SIMs come complete with graphically rich monitoring capabilities that provide flexible displays for every role in the organization. These graphical dashboards with role-based views ensure that security status is continually evaluated across the organization and critical issues get the attention they require.

Part E: Making a Log Review Program Apply to Policy

Streamlined Security

Prior to the introduction of SIM technology, businesses had no reasonable means of identifying whether or not they were under an attack until it was too late. But with the advent of SIM technology, businesses are discovering a number of important benefits. They are better able to better identify true threats to the network, as well as vastly increase communication and efficiency when responding to those threats. In many cases, SIM technology has allowed organizations to reduce their response time from hours to minutes. Just as importantly, SIM gives them the ability to automatically address many more threats with no additional headcount.

Meeting Compliance Requirements

Audit, compliance, and IT governance are major requirements for all enterprises. The need to centrally collect, monitor, respond and report on security event logs is more important than ever. A strong SIM technology can automate time-consuming processes related to proving compliance to regulations such as SOX, GLBA, FISMA, HIPAA and PCI.

By centrally collecting, storing and monitoring security event data, best-of-breed SIM systems can help deliver one-click compliance reporting that provides relevant data in a relevant format. SIM allows users to demonstrate the ability to monitor, respond and mitigate risk, a key compliance requirement. Some advanced SIM products can also separately monitor and report on events that involve regulated systems while driving accountability and awareness for all stakeholders.

Thwarting Insider Threat

A good SIM can serve as a central point of truth for user activity. Through the collection of operating system, application and other logs, SIM systems can monitor the network for violations and behaviors that indicate suspicious activity or a breach of acceptable use policy.

The best SIM systems feature enhanced ability to detect malicious insiders and inappropriate system usage through data models and analytic functionality. For instance, the system can integrate application usage to trend employee interaction with sensitive data and immediately alert the security team to anomalies. It can track system changes and identify at-risk employee behavior. And it can create an audit trail for privilege changes on critical servers.

Part F: Joining Security Information with Business Risk

SIM in Action

Workflow and business relevance are often forgotten parts of a SIM implementation. By integrating these two factors in a carefully conceived way, organizations can benefit from improved risk management and enjoy the most automation possible. This can also help speed you on your way to fulfilling audit points in a tight time-frame by demonstrating implementation of centralized log and compliance related log review.

Organizations can integrate business relevance into a SIM solution that supports this data type in two ways:

- If the organization has an asset database, this information may be imported into the SIM system. However, organizations must qualify whether assets have been appropriately classified using an asset classification structure such as FIPS-199.
- If the organization does not have an asset database, it is best to start simply and set up a plan to periodically review the applicability of the existing asset classification structure. Starting simply is important because organizations will quickly find more applications for their SIM solution over time and

the original asset classification structure may be overkill or unnecessary based on an actual implementation.

Workflow, if the SIM solution supports it, should be based on supporting processes relating to risk management, security monitoring, incident response, compliance and audit. Customizing the system to automatically route notifications, open cases, and send information to external system delivers a degree of automation that can save countless hours every day and will also serve as proof to auditors for demonstrating due diligence of process. In the beginning, start simply by identifying less than 20 lower level use cases and identifying appropriate procedures.

Conclusion

We live in challenging times. Corporate computer networks are continuously under siege by hackers and malicious insiders eager to exploit any and every vulnerability. A seemingly endless stream of government regulations has also raised the stakes when it comes to protecting confidential data. By using SIM technology to transform event logs into business-relevant information, organizations can protect themselves and their customers while complying with new requirements.

About the Author

Gretchen Hellman joined [ArcSight](#) as the Senior Manager of Product Marketing with broad experience in helping companies of all industries meet their security management and regulatory compliance objectives. After gaining direct experience as a consultant specializing in security management and regulatory compliance, Gretchen has worked with technology vendors and their customers to deliver practical solutions to the complex security and compliance problems facing today's IT security groups. Gretchen is a frequent speaker in the areas of security standards and control frameworks, regulatory compliance strategies, security policy, security information management, and security technologies. She holds a B.S.E.E. from Santa Clara University.

About ArcSight

ArcSight, a leader in Enterprise Security Management (ESM), provides real-time threat management and compliance reporting yielding actionable insights into your security data. By comprehensively collecting, analyzing and managing security data, ArcSight ESM™ enables enterprises, government organizations and managed security service providers to centrally manage information risk more efficiently. ArcSight's customer base includes leading worldwide companies across many verticals—and more than 20 of the largest U.S. federal agencies.