

Realtime
publishers

The Essentials Series

Security Information Management

sponsored by

SecureWorks®

by Dan Sullivan

Article 1: The Business Case for Security Information Management.....	1
Understanding and Mitigating Risks.....	1
Assessing Risks.....	2
Protecting Business Operations.....	2
Satisfying Requirements and Maintaining Compliance.....	3
Defending the Network.....	4
Ability to Detect Targeted Attacks.....	4
Respond Faster to Attacks.....	4
Improve Other Controls.....	4
Tools to Prioritize Resources and Spending.....	5
Long-Term Benefits of SIM.....	5
Summary.....	6
Article 2: Foundations of Security Information Management.....	7
Data Collection and Pre-processing.....	7
Data Collection Methods.....	8
Pre-Processing and Data Normalization.....	8
Data Analysis and Incident Identifications.....	9
Incident Response.....	11
Challenges and Best Practices.....	12
Summary.....	12
Article 3: Making Security Information Management Work for Your Organization..	13
Common Challenges with SIM Technology.....	13
Options for Addressing SIM Challenges.....	15
Selecting the Best Option for Your Organization.....	17

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This series was downloaded from Realtime Nexus—The Digital Library for IT Professionals. All leading technology eBooks and guides from Realtime Publishers can be found at <http://nexus.realtimepublishers.com>.]

Article 1: The Business Case for Security Information Management

Executives and managers have long had constant demands for their attention, from strategic planning and operation efficiencies to financial management and human resource issues. Today, we have to add security information management (SIM) to that list. It is a mistake to assume that information security is a technical problem best left to IT professionals; it is both a technical and a business challenge that demands a broad range of expertise and business acumen to address.

Information security is fundamentally a set of business and technical practices designed to protect an organization's information assets and infrastructure. This first article in this series on SIM discusses the need for a risk management approach to information security and describes for executives and non-IT managers a framework for understanding security risks and formulating a response based on business requirements. IT professionals will find the risk management approach fits well with IT operations and management practices. The discussion of this bridge between the business and technical approaches to SIM is organized around three key topics:

- Understanding and mitigating risks
- Prioritizing resources and spending
- Realizing the benefits of SIM

SIM begins with the principle that you cannot protect assets you do not understand.

Understanding and Mitigating Risks

The practice of risk management has developed in business as a rational, methodical way to understand the extent and types of risks we face and to optimize how we allocate resources to protect assets. This leads to a two-phase approach: assess risks and implement defensive measures.

Assessing Risks

Businesses face a wide array of risks, including changing market demands, inflation, industry consolidation, and fluctuation in the labor supply, to name several. IT and information assets face other types of risks as well, including, but not limited to:

- Data loss and disclosure of private and confidential data
- Loss of system availability due to network-based attacks
- Stolen computing, storage, and network resources due to botnets and other forms of malicious software
- Degraded network and application performance because of large volumes of unauthorized traffic (that is, spam)
- Loss of data integrity due to malicious tampering with data

Cyber-threats are so pervasive that an array of government and industry regulations has been established to ensure that businesses adequately protect the confidentiality and integrity of essential data and systems. Some of the most well known include the Payment Card Industry Data Security Standard (PCI DSS) for protecting payment card data, the Gramm-Leach-Bliley Act (GLBA) security requirements for financial services, the Critical Infrastructure Protection (CIP) standards for safeguarding power-generation utilities, and the Health Insurance Portability and Accountability Act (HIPAA) for securing sensitive health information. When assessing risks, one must consider how to both protect business operations and remain in compliance.

Protecting Business Operations

To properly manage risks, we must first understand the assets in an organization and the threats to those assets. Assets include physical infrastructure, such as workstations, servers, laptops, routers, storage arrays, and other hardware components. We must also protect intangible assets such as databases, applications, and confidential information. With an inventory of all IT and data assets, we can conduct a simple exercise: imagine if that asset were compromised or no longer available; could your business still function, and if so, how?

Consider several examples:

- If a Customer Relationship Management (CRM) database were unavailable because the server were infected with malware and the entire operating system (OS) and application stack had to be reinstalled, what parts of your business would be affected?
- If an email server were unavailable because allocated storage had been consumed by inordinate amounts of spam flooding the system, what business functions would be impaired?
- If an employee launched an insider attack to steal customers' credit card information, how would you detect the theft and prevent it? If it were not prevented, how would the business protect its customers and retain their business? What legal ramifications or liability would you face?
- If a botnet had infected a sizeable percentage of the business' workstations, how much IT staff time would be required to recover, what other operations would be delayed, and what is the opportunity cost to the business of having to mitigate this threat?

In each of these cases, one could readily argue that prevention is less costly than recovery. The potential for disrupted business is not the only cost of poor risk management; there are also concerns about compliance.

Satisfying Requirements and Maintaining Compliance

Government and industry regulations often require not only security controls but also the ability to demonstrate the effectiveness of those controls. This latter requirement often involves log management in practice. For example, PCI DSS requires companies to track and monitor access to cardholder data and network resources; GLBA specifies that banks must monitor networks and hosts for policy violations, misconfigured devices, and anomalous behavior on the network; HIPAA's technical requirements dictate the need for access and audit controls on protected health information. SIM provides comprehensive log management and can readily meet compliance requirements by aggregating log data and streamlining reporting.

Defending the Network

Defending a network is a multi-faceted operation. A defense-in-depth strategy, which incorporates multiple, varied security measures in a layered approach, is often used in network defenses. There are many forms of attacks, and the most sophisticated malware and directed attacks exploit multiple vulnerabilities. Analogously, network managers and systems administrators can use a SIM approach to coordinate multiple countermeasures to protect a business' information assets, ensure compliance with relevant regulations, and enable defense-in-depth measures.

A coordinated approach to collecting and analyzing security information provides several advantages over more isolated management approaches. Those advantages include the ability to detect targeted attacks, respond more quickly to attacks, and improve other technical controls.

Ability to Detect Targeted Attacks

Businesses can be the victim of targeted attacks—not just indiscriminate malware attacks—against their particular systems. These attacks take advantage of specific vulnerabilities in a network and its applications. For example, an attack may exploit a SQL injection vulnerability in a Web application, cause a buffer overflow on a network service running on an improperly configured server, or use a simple dictionary attack to discover administrator passwords on key servers. With a consolidated reporting system, information on the state of servers, firewalls, Intrusion Prevention Systems (IPSs), and applications can provide a comprehensive picture of your overall security posture. The ability to detect targeted attacks and other anomalous behavior is required by regulations such as GLBA and HIPAA.

Respond Faster to Attacks

Manually reviewing log files and alerts from different data sources takes time. Automatically collecting and correlating that data can help to significantly reduce the time to detect and diagnose an attack. This in turn reduces the time to mitigate the threat, minimizing the window attackers have to steal data or compromise systems.

Improve Other Controls

The information provided by a SIM system is a valuable resource for understanding the effectiveness of other security controls. For example, weaknesses in authentication systems may become apparent from log data indicating administrator activities on the financial system outside of normal business hours. This information in turn can motivate changes to server deployment and patch management processes. SIM information could also help identify firewall rules that can be tightened or IPS policies the need refining.

These advantages of SIM aid the needs of both the business and the technical managers.

Tools to Prioritize Resources and Spending

SIM systems can help business planning by providing tools and information to help assess the risk to assets. SIM applications can provide real-time risk management data, especially with regard to the level of activity for specific threats. For example, if the SIM system indicates a particular group of servers most subject to attack. These servers could then become top priority for patching because they are the most likely to be attacked. SIM systems are also useful for day-to-day management operations as well as long-term strategic planning. Operational metrics, such as the number of malware infections or the number of login failures, are useful for spotting events outside of normal, baseline ranges.

Long-Term Benefits of SIM

SIM practices may appear primarily defensive in nature, but they also enable more reliable business operations. When line managers and executives are confident their operation procedures can and will function under a range of circumstances, these processes will be more adaptive to the changing demands of the market:

- Would an executive be willing to sign off on a new project to launch a Web-based customer service portal if she was not sure the customer database was secure?
- Would a CIO allow employees to use their personal mobile devices to access corporate email and databases if those devices were not properly secured?
- Could an IT administrator support remote networks without proper monitoring and management tools?

SIMs and other security measures reduce the likelihood that concerns about security will curtail innovation.

As the demands for compliance grow, businesses need tools to monitor and respond to security incidents and to document and report on their ability to respond. SIMs can help reduce the time and staff resources required to meet immediate compliance requirements as well as facilitate compliance over the long term.

Perhaps the most significant cost justification for a SIM investment is saving the cost of a single data loss incident:

- A 2007 study by the Ponemon Institute in the United States found, on average, companies lost \$197 per lost record, up from \$182 per record lost in 2006.
- A 2007 Gartner study found the cost of complying with PCI was about \$16 per account.

In short, the cost of compliance can range roughly from as little as one-twentieth to one-fifth the cost of non-compliance.

Average costs per record can sometimes hide the magnitude of breaches. For example, a breach of customer data at TJX stores appears to have cost the retailer more than \$250 million. A breach at Fidelity National Information Services, Inc. in 2007 may have exposed 2.3 million bank and credit card records, and another at Hannaford Bros. Co from late 2007 to early 2008 may have exposed 4.2 million credit card numbers and related data. Given the cost per record and the number of records lost in some data breaches, the ROI on SIM can be substantial.

Summary

SIM is a business enabler. A secure information infrastructure is required to function in today's business world, but it must be maintained in a timely and cost-effective manner. This in turn requires the sound security strategy and cost-effective monitoring and data analysis that is enabled by SIM systems. CIOs, CSOs, and other IT professionals formulate security strategies by understanding and mitigating risks and prioritizing resources. SIM technologies are a key enabler for such strategic planning, they provide immediate benefits to day-to-day operations, and they can help avoid costly security incidents.

Article 2: Foundations of Security Information Management

Security information management (SIM) is a multi-step process that, broadly speaking, consists of data collection, data analysis, and incident response. Each of these steps consists of a complex series of operations. In this, the second of three articles about SIM, we examine the operational details of security information management. The article begins with a technical discussion of the operational issues in SIM but addresses organizational issues as well. Specifically, this article covers:

- Data collection and pre-processing in SIM systems
- Data analysis and incident identifications
- The role of SIM in incident response
- Challenges and best practices in SIM

We begin with basic monitoring and data collection.

Data Collection and Pre-processing

Security-related information can be collected from a wide range of sources throughout the network:

- Gateway devices, such as firewalls and routers
- Network appliances, such as Intrusion Prevention Systems (IPSs), antivirus appliances, and content filters
- Application servers, Web servers, database servers, and other core applications that log event information

Before it can be analyzed, this data must be collected in a central staging area and properly normalized.

Data Collection Methods

SIM systems typically use a push data collection method in which log data is sent to a SIM collection appliance using one or more methods. Commonly supported protocols such as Syslog, Simple Network Management Protocol (SNMP), or the Simple Mail Transport Protocol (SMTP) can provide near real-time updates. The key advantage of these protocols is that they are widely supported; unfortunately, they may not provide some of the useful contextual data available to the source system.

Some devices, such as Windows Servers, do not forward event logs natively, and in these situations, software agents must be installed to enable log collection. This introduces another component that must be maintained, adding to the complexity of SIM. In addition, agents are device specific, so organizations with a wide array of devices in use will assume a substantial installation and management challenge.

A third method of data collection is via native application programming interfaces (APIs). These introduce more complexity than the simple log forwarding protocols but provide greater contextual detail than those protocols. They can, for example, provide packet decodes via an API giving details of the security context that triggered the IPS alert.

Pre-Processing and Data Normalization

Pre-processing is a general term used to describe the file manipulation and data normalization that is required to map data into a format the SIM system can manipulate. A SIM, for example, may have data from a firewall, an IPS, and an antivirus appliance all related to a single event; however, because the source systems are manufactured by three different vendors, even common data types may be formatted differently.

Although pre-processing modules extract and reformat data, normalization procedures ensure that data from different systems referencing the same kind of data all use a common frame of reference. For example, timestamps should be comparable between source systems even though each system has its own clock. Similarly, a physical device on the network could be uniquely identified by either a currently assigned IP address or a MAC address; using one identifier scheme makes the analysis operations less complex.

Synchronizing system clocks can be a challenge. One approach to solve this problem is to add a timestamp to an event when it arrives at the SIM appliance so that both the source device timestamp and the SIM appliance timestamp can be used to establish a common network time. Another challenge can arise when a single physical server runs multiple virtual machines. Information tied to a MAC address may need to be correlated with events in one of the virtual machines. Once these challenges are overcome and the raw data is in a standardized format, the data analysis stage can begin.

Data Analysis and Incident Identifications

Data analysis and incident identification is a three-step process:

- Aggregating and filtering events
- Correlating events of interest
- Assessing incidents

Source systems generate a great deal of data. Not all of these log entries and event notifications are relevant to determining whether an incident has occurred. One way SIMs deal with the problem of information overload is through filtering and aggregation.

Filtering is performed with two types of filter sets, positive and negative. Positive filters capture known malicious or suspicious events. These events should not occur under normal circumstances and need to be analyzed further to determine whether there is a threat. Negative rules eliminate known events that are expected under normal operating conditions and have zero chance of being a threat. Of course, events that have never been processed before fall into neither the positive nor negative category; these are considered “anomalous” and should be investigated immediately to determine whether they are threats and update filter sets accordingly. This ability to incrementally improve filter rules enables SIM systems to scale to the breadth of requirements in businesses today.

Aggregation methods are used to further consolidate events. For example, a firewall might generate details about a port scan of the perimeter firewall. Tens or hundreds of individual events documenting the scanning of each port is not useful to network managers, but a single event with an aggregate count and range of those ports scanned is actually useful information.

Once the significant events have been isolated, they are correlated to determine the sequence of events and identify potential attack patterns. For example, a file may be transferred to a server, a configuration file changed, and then a data file copied from the network. Correlation can occur along a number of dimensions in the data:

- Data contained in the event, such as source and destination IP addresses, device, event summary, and event time
- Asset data, such as types of applications running on devices
- Asset classification data, such as the business purpose of the device
- Vulnerability scanning results
- External intelligence data, such as provided by BuqTraq, CERT notices, and subscription feeds
- Time-related attributes, such as time of day and number of events in a given period of time

A series of individual or correlated events might trigger a logic rule indicating a possible breach. This pattern matching by is the last step in the process and the one that triggers an event notification that a significant event has occurred.

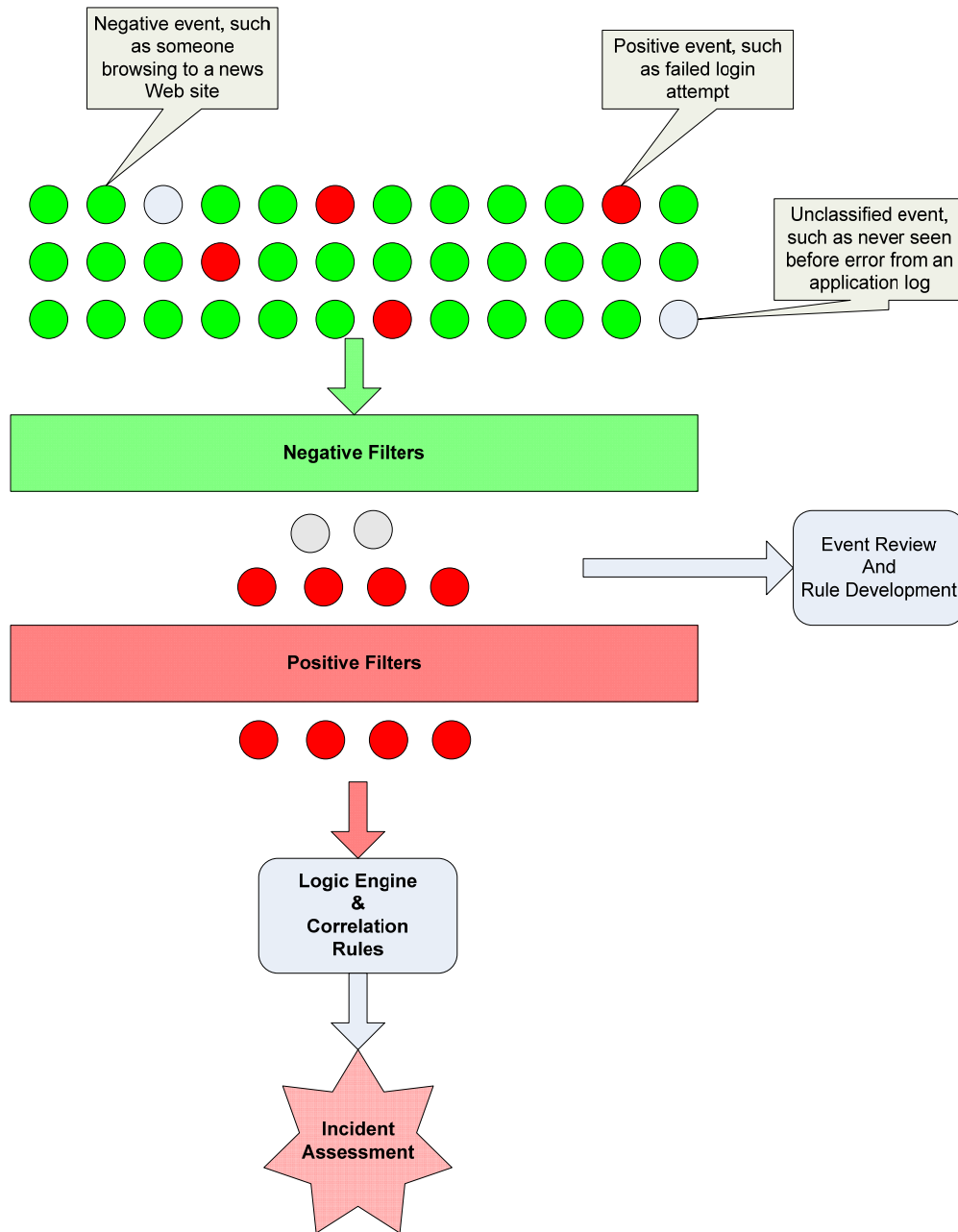


Figure 1: Large volumes of raw events are filtered to identify those that are significant and then to determine whether an adverse event has occurred.

Once an incident has been identified, IT staff should respond following an incident response plan.

Incident Response

Best practices dictate that you have an incident response plan in place rather than rely on *ad hoc* reactions to individual incidents. A common framework for incident response plans is the five-step cycle depicted in Figure 2. SIM practices and technologies can inform and improve all phases of incident response because a SIM system gives a comprehensive picture of events on the network.

Clearly, SIM's ability to collect data from diverse devices, filter irrelevant events, and correlate data support the detection phase of incident response. This is especially important because the sooner a breach or malicious event is detected and contained, the less chance of a costly loss.

See the first article in this series, "The Business Case for Information Management" for statistics on the costs of data breaches.

The monitoring services provided by SIMs also aid with the *contain, eliminate, and recover* phase to help ensure that all instance of malicious activity have been eliminated. Finally, in the *learn and adapt* phase, SIM data can provide forensic details that illuminate how a breach occurred and where additional security measures are required.

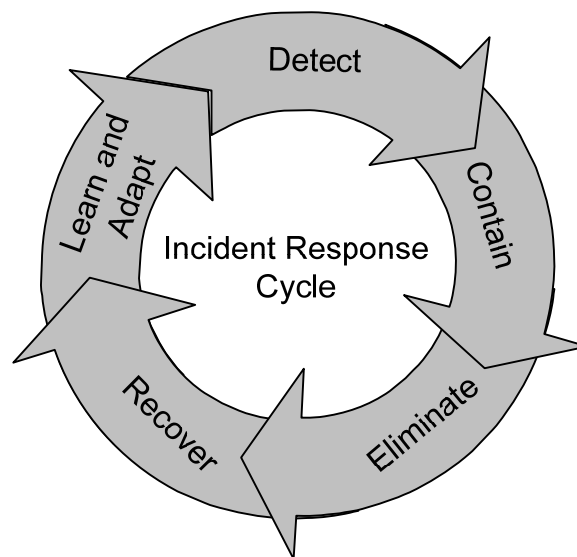


Figure 2: The incident response cycle brings a system back to operational state and leverages lessons learned to keep it secure.

Challenges and Best Practices

SIM is a practice that builds on other security measures and operations. Not surprisingly, the challenges to implementing effective SIM are shared by security practices as well.

SIM systems must scale to meet the volume of data generated on a network. Scalable performance can come from a number of areas, including improved filtering to reduce the number of events that must be analyzed, tuning incident detection rules to reduce the time required to analyze significant event patterns, and adding devices to load balance filtering and analysis operations.

IT staff face the challenge of staying current with the threat landscape. Cybercriminals and others attackers are constantly developing new techniques to avoid detection and exploit vulnerabilities. This situation demands that staff maintain adequate training and levels of expertise.

For additional details, see the third article in this series, “Making Security Information Management Work for Your Organization.”

Summary

SIM is a combination of technical and business processes. SIM includes data collection and pre-processing, data analysis, incident identification, and incident response as the major steps to controlling security breaches. It also includes long-term planning, incident response formulation, performance management, and training to ensure that adequate resources are in place to detect, remediate, and recover from security incidents.

Article 3: Making Security Information Management Work for Your Organization

Security information management (SIM) technology arose to address common problems with deploying multiple security systems and applications running within an organization. There is clearly a need for multiple systems, and this need has fostered the evolution of a defense-in-depth strategy that counters weaknesses in any security measure with the use of complementary controls. The most effective defense-in-depth approaches leverage different security systems to mitigate risks, in part by providing a comprehensive picture of the state of network security. Providing that picture is one of the many functions of SIM. Fortunately, businesses now have a number of options for deploying SIM technology.

In this, the third and final article in this series, we examine issues in deploying SIM technology. Specifically, we will examine:

- Common challenges with SIM technology
- Options for addressing these challenges
- How to select the best option for your organization

Of course, the needs of businesses and organizations will vary, so the goal of this article is to provide a framework for understanding common issues and options for effectively and efficiently addressing them. Of particular importance is choosing an appropriate implementation strategy, such as an in-house solution, an outsourced service, or an on-demand SIM service that combines the benefits of both.

Common Challenges with SIM Technology

SIM technology collects, analyzes, and reports on data from multiple point solutions. Each of the constituent systems has its own complexities and operational issues, so it is not surprising that consolidating their information with SIM systems presents challenges. Broadly speaking, we can categorize these challenges into three areas:

- Implementation challenges
- Information overload
- Unexpected management problems

As with other technologies, the difficulties can literally begin as soon as you open the box.

Implementation Challenges

Implementing a SIM system requires careful planning for successful installation and configuration. One needs to understand the data provided by source systems, which ranges from mundane issues, such as how log files are formatted, to more interpretive data, such as the meaning of different event types logged. There are also network-level considerations. For example:

- How will data be collected from source systems?
- How frequently will it be collected?
- How does one balance the need for timely updates of the SIM system with constraints on bandwidth and other network resources?

For those organizations with substantial staff SIM expertise and resources available, these issues can be readily managed. For others, an outsourced or on-demand service can provide the needed security knowledge.

In addition to coordinating functions with source systems, SIM systems administrators will have to tune rules regarding data analysis on an ongoing basis. System performance is hampered by inefficiencies in the rule base, which require varying degrees of restructuring from time to time. For example, a subset of rules may only apply if certain conditions are met; ideally those conditions should be evaluated only once, and if they are not met, the related rules should not be evaluated. Although SIM vendors will account for this type of situation as much as possible with their standard rule base, systems administrators will need to account for this need with customized rules. Once again, the availability of expertise is a primary consideration; on-demand solutions that provide SIM technology, a broad set of rules, and the ability to customize rules for your network may provide the best balance of benefits.

Information Overload

Another challenge to effective SIM is avoiding information overload. Security applications can generate a great deal of log and event data. Raw data, however, is of limited operational use to network administrators and systems managers. Instead, processed data that is derived from raw data and provides information about high-level events and appropriate response to those events is needed.

The problem of too much data and not enough information can occur when rules are too general. For example, capturing and reporting on every port scan of the network perimeter will provide overwhelming data. Data about targeted scans—for example, attempts to use a well-known port for a database listener—is much more useful, especially if it can be correlated with other events that indicate a targeted attack on a database server.

The flip side of this problem can reduce the amount of information generated. Narrowly defined rules can miss significant patterns in traffic and eliminate useful information in the name of avoiding information overload. The goal is to collect as much relevant information about an event as possible to provide maximum detail, and consolidate that information to reduce the time and effort required of an administrator to correlate separate pieces of information.

To summarize, the problem of information overload, filtering data, and distilling relevant data into actionable information is one that SIM administrators will continually face.

Unexpected Management Problems

The technical challenges of security are fairly well understood, or at least expected. There are business and organizational issues that are not always so obvious. The technical hurdles previously described come with costs that can be easily underestimated. This is especially the case with SIM implementations because organizations may have had limited experience with the tuning tasks and information overload containment entailed.

There will also be significant management overhead in the initial deployment stages. Several staff members with different expertise areas may be required to diagnose problems, tune rules, and analyze output. As business operations, services, and network configurations change, there will be changes in network traffic and related events. These will require further refinement of the SIM system.

Clearly, businesses implementing SIM technologies face a variety of difficulties, but at least there are options for addressing those issues.

Options for Addressing SIM Challenges

The options for implementing SIM include in-house solutions, outsourced, and on-demand solutions.

In-House SIM Solutions

With an in-house solution, businesses assume the full responsibility for implementing, configuring, and maintaining the SIM system. This requires that the organization hire or develop in-house expertise or use consultants to support the full life cycle of SIM.

The advantage of developing in-house expertise is that the staff may already have knowledge of the business environment and infrastructure. This could be especially useful with tuning and analyzing SIM system outputs. The disadvantage of this approach is the additional time and cost required to develop SIM expertise. The time to train can delay deployment and leave the network more vulnerable than it might otherwise be.

Consultants can provide expert assistance without delays for training. Of course, even with solid training, there are some things best learned by experience. Consultants can bring hard-earned lessons from previous engagements. The disadvantages of consultants are, first, they do not have in-depth knowledge of your business and, second, the costs can grow quickly with extended engagements.

Outsourced Solutions

Providing IT applications as a service is an increasingly popular model. Businesses can now purchase services ranging from Customer Relationship Management (CRM) and database applications to security and network management. One can even purchase specific security services, such as vulnerability scanning, on an as-needed basis. For the purpose of this discussion, we distinguish between outsourced and on-demand solutions.

An outsourced solution is one in which a service provider offers a SIM solution and retains control over the infrastructure underlying the service, the configuration and rule base used, and the analysts who monitor for threats. Fully outsourced providers also supply SIM analysts to monitor for threats. This model works well for customers who prefer a turnkey solution and do not require that their own staff shape policy and rules.

On-Demand Solutions

On-demand solutions are similar to outsourced solutions in that infrastructure is managed by the provider but customers have greater control over the policy and rules enforced and used by the SIM system. This model works well for customers who want to outsource infrastructure management while retaining control over higher-level decisions about SIM policy and rules. The advantages of an on-demand model include rapid implementation and ready scalability. Service providers already manage a service infrastructure, so deploying SIM operations to a new customer is a marginal change rather than a full-scale implementation of an in-house solution, saving the customer on implementation costs. This model can also scale to meet customer demands more cost effectively than an in-house solution because service providers offer advantages of economies of scale which result in cost savings to the customer.

The pay-for-use model common in software as a service also allows for more predictable expenditures and reduces the need for capital expenditures simply to start a SIM project. Another advantage of on-demand solutions is access to experts who can tune and help analyze SIM data. These providers also have access to diverse SIM deployments allowing them to identify threats and implement SIM rules for them faster than others with less breadth of visibility.

SIM Feature	In-House	Fully Outsourced	On-Demand
Customer free from infrastructure management issues		✓	✓
Customer control over policies and rules	✓		✓
Customer manages analysis	✓		✓
Customer specifies Service Level Agreements (SLAs)		✓	✓
Customer responsible for monitoring SIM alerts	✓		✓

Table 1: Considerations and options when choosing a SIM implementation method.

Selecting the Best Option for Your Organization

The choice between an in-house solution and a service provider can be decided based on several factors:

- Budget—Are capital funds available to implement a full-scale, in-house solution?
- Expertise—Does your staff have the time and technical knowledge to configure and tune a SIM system?
- Staffing—Will maintaining a SIM system in-house take IT staff from other support operations?
- Management concerns—Is your organization comfortable working with a service provider model?
- Experience—Does your management team have experience negotiating SLAs?

As is often the case with technology solutions, there are trade-offs. In the case of SIM systems, it is important to consider both technical issues—to ensure your solution meets your security needs—and business issues—to ensure you provide a sustainable solution that supports business operations. The on-demand method provides advantages of both the in-house and fully outsourced models and may offer the most adaptive approach for businesses that want to retain some control over their SIM system without assuming the additional burden of infrastructure management.

Download Additional Resources from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this series to be informative, we encourage you to download more of our industry-leading technology eBooks, video guides, and article series at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.