Realtime publishers

The Essentials Series:
Security Information Management

Making SIM Work for Your Organization

sponsored by

SecureWorks®

by Dan Sullivan

Copyright Statement

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.