

## **Security information management**

*Author: Curtis Franklin Jr. is senior analyst of the InfoWorld Test Center.*

SIM (security information management) products have become more accepted as critical components within the network security infrastructure. As such, understanding the criteria for selecting SIMs has become more important. Moreover, in a fast-evolving market segment [SIM becomes SEM (security event manager), becomes SI/EM, becomes ...], it's more important to understand the important architectural differences and implementation requirements than the industry acronyms and product names. A wave of consolidation has already begun to hit the SIM market, but the major issues and deployment criteria span brands and individual technologies.

### **What is a SIM?**

A SIM automates collection and analysis of information from all the security components in a network. Rather than having to look at logs and alerts from firewall, IDS, anti-virus, VPN, and other security systems, a security manager can obtain all of this information from a single SIM console. Some SIMs simply aggregate reports from these various components; others correlate the information to improve the quality of overall security information.

There are two key benefits to this data aggregation: First, it reduces the cost and improves the effectiveness of security monitoring. Second, it simplifies and improves reporting of security information for audits in support of regulatory compliance. HIPAA, Sarbanes-Oxley, GLB, and FISMA -- and the consequences of noncompliance -- are prime driving factors in the increased deployment of SIMs.

It's important to briefly consider the difference between SIM, SEM, and anomaly detection software. SIM systems tend to collect information of all sorts from security components. That information includes events, alerts, ongoing status, and full network-traffic capture.

SEM products, on the other hand, tend to focus on the events and alerts in an attempt to improve on IDS (intrusion detection system) functionality. Anomaly detection takes a somewhat different approach: It initially surveys the network to establish a baseline of condition and behavior, then reports on any changes to these patterns.

Some SIMs have adopted elements of anomaly detection in their operation. In fact, the functions of all three product types are rapidly converging. The market movement is clear; the label that will be applied to the resulting class of product is yet to be decided.

### **SIM-buying criteria**

***How does the SIM get information?*** The basic question is whether the SIM depends on agents (sometimes called monitors or probes) installed around the network, or does it take its information from the log files and SNMP events generated by the existing network infrastructure. If the product depends on its own agents, it can very tightly tie the input stream to event processing, which can make it somewhat more efficient. If the product depends on log files and SNMP events, it can cast a much wider net (though you must be sure that it can handle the log files produced by *your* infrastructure devices), and it can be less expensive to deploy.

Some products use a combination of the two architectures, accepting log files and using their own dedicated agents. You must look at the architecture of your network to know whether one approach or the other will provide the most visibility to the SIM.

***Where will the information be processed?*** In a network of any size, the SIM will be dealing with a large quantity of data. Precisely where and how the data is processed will be key to knowing whether a particular SIM can keep up with the data generated by your network. Almost all SIMs have two primary components for the creation and presentation of information: the SIM appliance itself and a dashboard application running on a remote workstation. If all the information is processed in either the appliance or the dashboard workstation, performance can become an issue when either network traffic or incidents become high in density. Ask about where data is processed and whether the processing is split between two (or more) systems. Delayed security information can result in falling victim to an attack that you might have survived.

***How will the information be correlated?*** All SIMs gather information from the sources within the network. Some will gather information from external sources as well, ranging from public threat identification services to proprietary correlation networks. Beyond eliminating the need for your security engineer to open 93 windows on his or her workstation just to keep up with log files, a SIM, to a great extent, adds value with its capability of finding patterns in network traffic. This activity requires two primary traits: the capability of gathering data from a various places and the intelligence to turn all that data into meaningful information. Both are critical. Just as the SIM must draw information from all of the important components of your network, the correlation data must come from sources you trust.

***How are reports generated?*** It's one thing to be notified that unauthorized activities are happening on the network. It's another thing entirely to convince less security-savvy network management to do anything about it. You want your SIM to be capable of generating reports to support your call for action -- and to generate them quickly. If the product comes with prepackaged reports that you can modify to provide the information specific to your organization and incident, then you're way ahead of the game.

Prepackaged reports are critically important time-savers when it comes to regulatory-compliance audits. If you know the format your auditing agency requires, then by all means ask whether those reports are included with your candidate SIM. Regulatory compliance audit reports could, by themselves, justify the purchase of a SIM system.

***How can you look at highlighted incidents?*** Reports are important in many situations, but for day-to-day security analysis, you'll spend much more time interacting with a security dashboard. A clean, well-organized dashboard and the ability to drill into reported incidents by time, severity, and type will mean the difference between productivity and frustration. How easily can you highlight a particular time period and analyze traffic by the criteria that you specify? How easy does the correlation engine within the client make it to look for patterns within a specified time? Is it effortless or difficult to look at traffic or interactions between specific addresses or types of clients?

With just about any product, you'll want a dashboard that has an initial set of analysis screens that get you started in a meaningful way. You'll also want something with easily customized screens and automated analysis runs to meet your needs.

***How can you share information with other applications?*** A SIMs is, without question, a powerful part of a security infrastructure, but it can't do it alone. You'll need other hardware and software to deal with the incidents discovered by the SIM, and life will be easier if the SIM itself can handle some of the interaction with those other pieces of infrastructure. As you're looking at SIMs, think about how you want the humans in the security hierarchy to work with the automated systems. Do you want the systems to take care of as much as possible, then notify staff as to what has been done? Or do you want the humans to keep their hands on the controls while the systems provide intelligent help?

Some SIMs will work in either of these ways -- or in both, as you begin with humans in control and gradually give more authority to the system as you gain confidence in its capabilities. Ask the vendors about which model they follow so that you can zero in on those that match your deployment expectations.

***How easy is the SIM to install and configure?*** This is the big wild card. As with virtually any category of hardware or software, there are products that are relatively easy to install, and there are some that will occupy your every waking moment for far too long. In most cases, deploying a SIM will break down into two lengthy tasks: arranging for the SIM to gather information from the network, and arranging for you to glean information from the SIM.

Getting information to the SIM varies in complexity depending on whether the SIM is collecting log files, gathering data from its own network of probes, or both. Initial efforts may be more or less dependent on how actively the SIM gathers its basic information. Does the SIM initiate scans of devices on the network, or does it simply sniff the traffic stream for events, assets, and suspicious traffic patterns?

In similar ways, the effort involved in configuring security monitoring and analysis can vary greatly depending on the degree of automation built into the SIM's installation routine. Some SIMs will put themselves into a configuration that's minimally useful by default. Others require you to step through an extensive setup routine. The payoff to this greater time investment is the system will, from the get-go, gather information tailored to your needs.

### **SIM vendors and solutions**

This list is not intended to be exhaustive, and owing to merger and acquisition activity in the industry, it may go out of date without notice.

#### **ArcSight**

Solutions: [ArcSight ESM](#); [ArcSight Interactive Discovery](#); [ArcSight Pattern Discovery](#)

#### **Cisco**

Solution: [CiscoWorks Security Information Management Solution \(SIMS\)](#)

#### **Computer Associates**

Solution: [CA Security Command Center](#)

#### **eIQnetworks**

Solution: [SecureVue](#)

**Enterasys**

Solution: [Dragon Security Command Console](#)

**High Tower**

Solution: [SEM 3200](#)

**netForensics**

Solution: [nFX SIM One](#)

**NitroSecurity**

Solution: [NitroView ESM](#)

**Novell**

Solution: [ZENworks Endpoint Security Manager](#)

**RSA**

Solution: [enVision Platform](#)

**Symantec**

Solution: [Symantec Security Information Manager](#)

**TriGeo**

Solution: [TriGeo Security Information Manager](#)