Gartner Research

Publication Date: 29 May 2009 ID Number: G00167819

Critical Capabilities for Security Information and Event Management Technology

Mark Nicolett

This research will help managers responsible for implementing security information and event management (SIEM) solutions to evaluate products from 11 of the major vendors in the segment. It outlines three major use cases and details the functions that managers should look for when assessing products, and then scores the 11 vendors' products on specific functions as they apply to the three use cases.

Key Findings

- Security event management (SEM) helps IT security operations personnel identify and be more effective in responding to external and internal threats.
- Security information management (SIM) provides reporting and analysis of data to support regulatory compliance initiatives, internal threat management and security policy compliance management.
- Gartner has defined nine major capabilities provided by SIEM technologies.
- Five critical capabilities differentiate management products for the three major use cases: log management, compliance reporting, SEM, deployment and support simplicity, and user and resource access analysis.

Recommendations

- Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of SIM vs. SEM capabilities, ease and speed of deployment, acquisition cost, the IT organization's support capabilities, and integration with system and application infrastructures.
- When developing requirements, include stakeholders from internal audit, compliance, IT security and IT operations.
- Develop a two- to three-year road map for all functions that will influence buying decisions for the initial implementation.

Introduction

SIEM technology is used to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for regulatory compliance and forensics. SIEM products provide SIM and SEM. Many Gartner clients need to implement SIEM technology to satisfy regulatory requirements — for example, log management for the payment card industry (PCI) or privileged user reporting for Sarbanes-Oxley (SOX). Our clients generally recognize that these compliance-funded projects are also an opportunity to improve security monitoring and incident management capabilities. This research will help organizations define their requirements and select technology (see "Magic Quadrant for Security Information and Event Management").

Product Class Definition

SIEM technology is composed of two main functions:

- SIM provides log management — the collection, reporting and analysis of log data (primarily from host systems and applications, and secondarily from network and security devices) — to support regulatory compliance reporting, internal threat management and resource access monitoring. SIM supports the privileged user and resource access monitoring activities of the IT security organization, and the reporting needs of the internal audit and compliance organizations.
- SEM processes log and event data from security devices, network devices, systems and applications in real time to provide security monitoring, event correlation and incident response. SEM supports the external and internal threat monitoring activities of the IT security organization, and improves incident management capabilities.

Critical Capabilities Definition

SIEM technology can be deployed to support three primary use cases: compliance reporting, threat management and a general SIEM deployment that provides support for both. Most organizations require a general SIEM deployment that implements capabilities in all three areas, but there is variation in use case priority and capability requirements.

SIEM technology provides a set of common core capabilities that supports all use cases, and also core capabilities that specifically support the threat management use cases or compliance reporting. Five of these are critical capabilities that differentiate SIEM technologies for major use cases. Many organizations will apply the technology broadly across their IT infrastructures and implement most of the core capabilities, but they typically start with a narrow deployment that implements a subset of functions to resolve a specific compliance gap or security issue. Gartner recommends developing a set of requirements that resolves the initial problem, but there should also be some planning for the broader implementation of SIEM capabilities in subsequent project phases. Developing a two- to three-year road map for all functions will influence the buying decision for the initial implementation.

Common Core Capabilities

A set of common core capabilities provides a foundation for SIEM products. Organizations should evaluate these capabilities for SIM *and* for SEM:

- **Event and data collectors:** SIEM products collect data via:
  - A combination of agents installed directly on the monitored device or an aggregation point, such as a "syslog" server
  - Invocation of the monitored system's command line interface
  - Application programming interfaces (APIs) provided by the monitored system vendor
- Filtering options at the source also are important methods of data reduction, especially for distributed deployments with network bandwidth constraints. A large percentage of organizations that have deployed this technology must integrate data sources that aren't formally supported by the SIEM vendors. SIEM products should provide APIs or other functions to support user integration of additional data sources. This capability becomes more important as organizations apply SIEM technology for application layer monitoring.
- **Correlation:** This establishes relationships among messages or events that are generated by devices, systems or applications, based on characteristics, such as the source, target, protocol or event type. Correlation is important for threat management (to track and analyze the progression of an attack across components and systems) and for user activity monitoring (to track and analyze the activity of a user across applications or to track and analyze a series of related transactions or data access events).
- **Event normalization and taxonomy:** A mapping of information from heterogeneous sources to a common classification. A taxonomy aids in pattern recognition, and it also improves the scope and stability of correlation rules. When events from heterogeneous sources are normalized, they can be analyzed by a smaller number of correlation rules, which reduces deployment and support labor. Normalized events are also easier to work with when developing reports and dashboards.
- **Scalable architecture and deployment flexibility:** Derived from vendor design decisions in the areas of product architecture, data collection techniques, agent design and coding practices. Scalability can be achieved by:
  - A hierarchy of SIEM servers — that is, tiers of systems that aggregate, correlate and store data
  - Segmented server functions — that is, specialized servers for correlation, storage reporting and display
  - A combination of hierarchy and segmentation
- **Deployment and support simplicity:** The compliance driver has extended the SIEM market to organizations that have smaller security staffs and more-limited system support capabilities. For these buyers, predefined functions and ease of deployment and support are valued over advanced functionality and extensive customization.

During the planning phase, many organizations underestimate the volume of event data that will be collected, and underestimate the scope of analysis reporting that will be deployed. An architecture that supports scalability and deployment flexibility will enable an organization to adapt its deployment in the face of unexpected event volume and analysis.

SIM Capabilities

Organizations that expect to employ SIEM technology to address security-related audit and regulatory compliance reporting issues should evaluate product support for two capabilities:

- **Log management:** Functions supporting the cost-effective storage and analysis of a large information store include collection, indexing and storage of all log and event data from every source, and the capability to search and report on it. Reporting capabilities should include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools.
- **User and resource access analyses:** This capability defines user access and resource access policies, and discovers and reports on exceptions. It enables an organization to move from activity monitoring to exception analysis. This capability is important for compliance reporting, fraud detection and breach discovery.

SEM Capabilities

Organizations that expect to employ SIEM technology to improve the internal and external threat management capabilities of the IT security organization should evaluate product support for four capabilities:

- **Real-time data collection:** Collect event data in near real time in a way that enables immediate analysis.
- **Security event console:** Real-time presentation of security incidents and events.
- **Real-time event correlation and analysis:** Monitoring, alerting and notification regarding threats and other security events in near real time.
- **Incident management support:** Specialized incident management and workflow support should be embedded in the SIEM product primarily to support the IT security organization. Products should provide integration with enterprise workflow systems.

Use Cases

The SIEM market is being driven by projects to resolve compliance issues, but most organizations also want to improve security monitoring and incident response. IT organizations evaluate and deploy SIEM tools for three primary use cases:

- **Compliance reporting:** The SIEM technology deployment is tactical, focused on specific compliance reporting requirements and a subset of servers that are material to the regulation. Log management is weighted heavily, because it provides the basic "check box" that a superficial audit would require. User and resource access reporting is important, because SIEM technology is commonly deployed as a compensating control for weaknesses in user or resource access management. The implementation time frame is typically short, so simplicity and ease of deployment are valued over advanced functions and the capability to heavily customize.
- **Threat management:** The IT security organization has obtained funding for an SIEM deployment by making the case for improved threat management and incident response capabilities. There's higher weighting to real-time event management, correlation, incident response workflow, and support for real-time network and security device event analysis.
- **General SIEM deployment:** In this use case, security has funding to close compliance gaps, but there's also a need to improve threat management and incident response capabilities. The SIEM technology must support rapid deployment for compliance reporting, and provide for subsequent deployment steps that implement SEM

capabilities. This use case is represented in the critical capabilities table as the "overall" category and score.

Critical Capabilities

Five critical capabilities differentiate vendor offerings for the three use cases (see Table 1):

- Log management
- Compliance reporting
- SEM
- User and resource access analysis
- Deployment and support simplicity

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Product Capabilities	Overall	Compliance	Threat Management
Log Management	20%	20%	10%
Compliance Reporting	15%	30%	5%
SEM	35%	5%	75%
User and Resource Access Monitoring	15%	20%	5%
Deployment and Support Simplicity	15%	25%	5%
Total	100%	100%	100%

Source: Gartner (May 2009)

Inclusion Criteria

In this research, we've included software products for evaluation, based on the following criteria:

- The products must cover the core SIEM functions.
- The products must have been in general availability and deployed in customer environments as of January 2009.
- The products must target the SIEM market segment and the security buying center.
- Gartner must have determined that the participants are the largest players in the market, in terms of installed base and revenue derived from SIEM products.

Based on these criteria, we've included products from 11 vendors: ArcSight, CA, Cisco, IBM, LogLogic, NetIQ, Novell, Q1 Labs, RSA (EMC), SenSage and Symantec.

Critical Capabilities Rating

Each of the products that meet our inclusion criteria has been evaluated on the five critical capabilities, on a scale from 1.0 to 5.0 (see Table 2).

Table 2. Product Rating on Critical Capabilities

Critical Product Capabilities	ArcSight ESM Plus Logger	CA SCC/ Log Manager	Cisco/ MARS	IBM/ TSIEM	LogLogic/ Appliances	NetIQ/ Security Manager	Novell/Sentinel and Identity Audit Package	Q1 Labs/ QRadar	SenSage/ Solution	RSA/ enVision	Symantec/ SSIM
Log Management	5.0	3.2	2.5	3.0	5.0	3.5	2.0	4.0	4.0	4.0	3.3
Compliance Reporting	4.5	3.5	2.5	3.8	4.0	3.5	3.0	4.0	4.5	4.0	2.5
SEM	4.5	2.3	3.3	3.3	3.0	3.0	4.5	3.6	3.0	3.3	3.5
User and Resource Access Monitoring	3.4	3.2	1.6	4.3	3.1	2.8	3.2	3.3	4.0	2.8	3.0
Deployment and Support Simplicity	3.5	2.0	4.0	2.5	4.5	3.0	2.7	4.0	3.5	4.0	3.5

Source: Gartner (May 2009)

To determine an overall score for each product in the use cases, the ratings in Table 2 are multiplied by the weightings shown in Table 1. These scores are shown in Table 3, which also provides our assessment of the viability of each product.

Table 3. Product Score in Use Cases

Use Cases	ArcSight ESM Plus Logger	CA SCC/ Log Manager	Cisco/ MARS	IBM/ TSIEM	LogLogic/ Appliances	NetIQ/ Security Manager	Novell/Sentinel and Identity Audit Package	Q1 Labs/ QRadar	SenSage/ Solution	RSA/ EnVision	Symantec/ SSIM
Overall	4.3	2.7	2.9	3.3	3.8	3.1	3.3	3.8	3.7	3.6	3.2
Compliance	4.1	2.9	2.7	3.4	4.1	3.2	2.8	3.8	4.0	3.7	3.0
Threat Management	4.4	2.5	3.1	3.3	3.3	3.1	4.0	3.7	3.3	3.4	3.4
Product Viability	Excellent	Good	Good	Good	Excellent	Good	Good	Excellent	Excellent	Excellent	Good
Product viability is distinct from the critical capability scores for each product. It is our assessment of the vendor's strategy and its ability to enhance and support a product over its expected life cycle.											

Source: Gartner (May 2009)

Vendors

ArcSight

ArcSight provides three SIEM offerings: Enterprise Security Manager (ESM) software for SEM, the ArcSight Express appliance for SEM, and the Logger line of log management appliances and collectors for SIM. ArcSight ESM provides capabilities needed for large-scale, SEM-focused deployments, but it's complex to implement and manage. ArcSight Logger is an easily deployed log management appliance that can be implemented "stand alone" or in combination with ArcSight agents and/or ESM. The capability to deploy Logger in combination with ArcSight agents provides additional options for normalized data analysis and application layer data collection. In April 2009, ArcSight announced general availability of ArcSight Express, an appliance-based offering for ESM designed for the midmarket with preconfigured monitoring and reporting, and simplified data management.

CA

During 2008, CA sold two SIEM products: CA Audit and CA Security Command Center (SCC). CA Audit provides basic log data collection and analysis for host systems, and CA has successfully sold it to identity and access management (IAM) customers as an audit enhancement. SCC provides SEM functions, but requires extensive customization and is not widely deployed. On 20 April 2009, CA announced general availability of CA Enterprise Log Manager, a software appliance that provides general log management, compliance reporting and analytics for applications, hosts, network devices and security devices. The product integrates with CA's IAM portfolio and is intended as a replacement for CA Audit.

Cisco

The security Monitoring, Analysis and Response System (MARS) is oriented to network SEM, and Cisco continues to position MARS as a component of its self-defending network strategy. MARS is narrow in its data source support in many areas, and Cisco has not expanded the scope of monitoring. Cisco MARS can be deployed for SIM and compliance reporting use cases that don't require source support beyond MARS limitations or extensive report customization.

IBM

IBM has three SIEM offerings: (1) Tivoli Compliance Insight Manager (TCIM), which is primarily oriented to user activity monitoring and compliance reporting; (2) Tivoli Security Operations Manager (TSOM), which is primarily oriented to SEM; and (3) Tivoli Security Information and Event Manager (TSIEM). TSIEM is a loose integration of TCIM and TSOM that provides event management, log management and compliance reporting. The integration among the products enables them to share a subset of events and also enables consolidated reporting across the products. IBM positions SIEM as a component of its broad security and operations software and service portfolio, and is focusing its SIEM technology development efforts on identity and access audit, data and application security, and z/OS security. IBM recently announced IBM Tivoli Identity and Access Assurance — an integrated bundle of IAM and SIEM technology.

LogLogic

LogLogic has extended its line of log management appliances to include full-function SEM and database activity monitoring (DAM). The core LX, ST and MX appliances provide log management functions and reporting for regulatory compliance, and for some operations use cases. The log management appliances have been frequently installed as a data collection and analysis tier in conjunction with SEM-focused products. The new SEM capabilities are an

implementation of technology from the Exaprotect acquisition (integrated as licensed technology before the acquisition closed) on a new LogLogic appliance — LogLogic Security Event Manager. LogLogic's Database Security Manager is a data collection and analysis appliance that uses agent technology that provides monitoring and virtual patch capabilities.

NetIQ

NetIQ Security Manager software is primarily oriented to SIM, user activity monitoring and compliance reporting. The software is easily deployed for host log monitoring, and NetIQ also provides an optional log management and archive component. The technology is sometimes deployed for network and security device sources. NetIQ's agents provide a comprehensive out-of-the-box Windows system and Active Directory monitoring. The company also offers an optional component — Change Guardian, which provides real-time file integrity monitoring for Windows systems and is integrated with Security Manager.

Novell

Novell is primarily focused on using SIEM to provide activity monitoring to its IAM customers. Sentinel (acquired in 2006) was originally designed for large-scale SEM-focused deployments. However, it is not well-suited for use cases that require simple deployment, or those oriented toward log management. At the time of this evaluation, Novell was planning the release of two enhancements: (1) the Sentinel 6.1 Rapid Deployment option — intended to provide simplified deployment and support (2Q09 release); and (2) Sentinel Log Manager — a log management tier for Sentinel (release planned later in 2009). Late in 2008, Novell released the Novel Identity Audit Package, which provides log management and reporting for Novell's IAM products. We have not been able to speak with reference customers for the new product. Novell also provides the Compliance Management Platform — an integrated bundle of IAM and SIEM technology.

Q1 Labs

The Q1 Labs QRadar appliance line provides a combination of SIEM, log management and network behavior analysis. QRadar Simple Log and Information Management (SLIM) is a log management appliance that can be upgraded to full SIEM capabilities. The QRadar technology provides an integrated view of the threat environment using NetFlow and direct network traffic monitoring, in combination with host activity monitoring and reporting from log data. The vendor has actively pursued deployments that require user-oriented monitoring and deployments that are compliance-focused. Q1 Labs also positions QRadar as a competitive alternative to Cisco MARS, and licenses the technology to some Cisco competitors (such as Juniper Networks and Enterasys).

RSA (EMC)

RSA, the Security Division of EMC, offers the enVision appliance, which provides a combination of SEM, SIM and log management. Although enVision has not been as capable in SEM as best-of-breed (and more-complex) point solutions, it has provided function in all three areas that was "good enough" for common use cases in an appliance form factor that is easy to deploy. In March 2009, RSA released enVision v.4, which has improved correlation capabilities for external threat management, privileged user monitoring and system monitoring. New correlation rules fully use the enVision taxonomy (as opposed to referencing source-level events).

SenSage

SenSage technology has been widely deployed for use cases that require analytics and compliance reporting against a large log event data store. SenSage provides explicit audit support for multiple packaged applications, and the company has OEM arrangements with HP

(Compliance Log Warehouse) and Cerner (healthcare applications). Version 4 of SenSage (released in 2008) has addressed limitations in real-time collection and event management capabilities, and we have been able to validate production deployments. Version 4 also delivered improvements to the user interface that ease deployment and administrative tasks, and has also improved the usability of report generation functions.

Symantec

The Symantec Security Information Manager (SSIM) soft appliance provides SIM and SEM capabilities, and it can be used to implement log management functions. The company has focused on the use of its DeepSight real-time security intelligence data to dynamically build monitoring for current external threats. Symantec provides integrations between its Security Endpoint Protection (SEP) and SIEM technologies. Symantec has managed service offerings that use the soft appliance for on-site data collection and analysis. SSIM implements a set of predefined queries that can be used to generate compliance reports for all the common regulations, but it does not provide out-of-the-box predefined reports. Symantec plans to release more predefined report content later this year.

BOTTOM LINE

SIEM tools enable user and resource access monitoring and reporting to satisfy audit requirements and SEM for improved threat response and incident management. Organizations must determine the relative importance of SIM vs. SEM requirements for their deployments, and evaluate products with regard to support requirements vs. internal support capabilities. Organizations evaluating SIEM tools should begin with a requirements definition effort that includes IT security, internal audit, compliance and IT operations.

Critical Capabilities Methodology

"Critical capabilities" are attributes that differentiate products in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

This methodology requires analysts to identify the critical capabilities for a class of products. Each capability is then weighted in terms of its relative importance overall, as well as for specific product use cases. Next, products are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities overall, and for each use case, is then calculated for each product.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor: most or all defined requirements not achieved

2 = Fair: some requirements not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

Product viability is distinct from the critical capability scores for each product. It is our assessment of the vendor's strategy and its ability to enhance and support a product over its expected life cycle; it is not an evaluation of the vendor as a whole. Four major areas are considered: strategy,

support, execution and investment. Strategy includes how a vendor's strategy for a particular product fits in relation to its other product lines, its market direction and its business overall. Support includes the quality of technical and account support as well as customer experiences for that product. Execution considers a vendor's structure and processes for sales, marketing, pricing and deal management. Investment considers the vendor's financial health and the likelihood of the individual business unit responsible for a product to continue investing in it. Each product is rated on a five-point scale from poor to outstanding for each of these four areas, and it is then assigned an overall product viability rating.

The critical capabilities Gartner has selected do not represent all capabilities for any product and, therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making an acquisition decision.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner