LICENSED FOR DISTRIBUTION

Gartner

Magic Quadrant for Security Information and Event Management

24 May 2012 ID:G00227899

Analyst(s): Mark Nicolett, Kelly M. Kavanagh

VIEW SUMMARY

Broad adoption of SIEM technology is driven by security and compliance needs. Targeted attack discovery requires effective user activity, data access and application activity monitoring. Vendors are testing demand for broader-scope solutions.

Market Definition/Description

The security information and event management (SIEM) market is defined by the customer's need 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. The vendors that are included in our analysis have technologies that have been designed for this purpose, and they actively market and sell these technologies to the security buying center.

SIEM technology aggregates the event data produced by security devices, network devices, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data. Event data is combined with contextual information about users, data and assets. The data is normalized, so that events from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring, user activity monitoring or compliance reporting. The technology provides real-time security monitoring, historical analysis, and other support for incident investigation and compliance reporting.

Return to Top

EVIDENCE

[1] "Critical Capabilities for Security Information and Event Management."

[2] "Toolkit: Security Information and Event Management RFP."

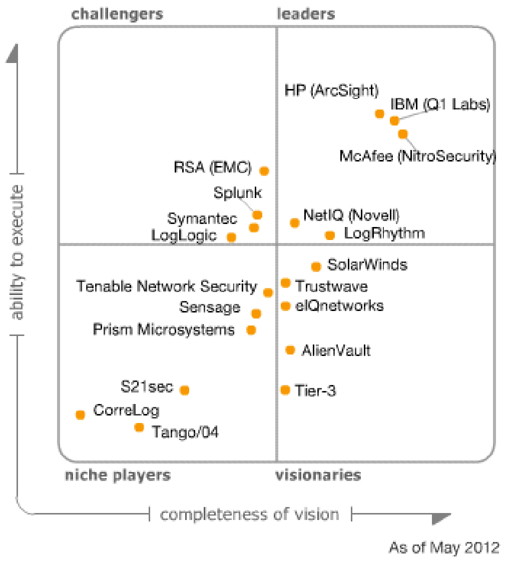
[3] Based on 300 inquiries during 2011 from end-user clients with funded SIEM projects.

[4] Based on surveys of 24 SIEM vendors.

[5] 2012 Data Breach Investigations Report from Verizon Business Systems.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2012)

Return to Top

Vendor Strengths and Cautions

AlienVault

The foundation for AlienVault's security management solution is Open Source SIM (OSSIM), which provides SIEM, vulnerability assessment, network and host intrusion detection, and file integrity monitoring. AlienVault markets and supports commercial software or appliance offerings that extend OSSIM with scaling enhancements, consolidated administration and reporting, and multitenanting for managed security service providers (MSSPs). There are three packaged offerings: AlienVault SIEM Pro (SIEM capabilities), AlienVault Compliance Management (SIEM plus selected additional tools enabled) and AlienVault Unified Security Management (SIEM plus all tools enabled).

In 4Q11, an experienced management team was recruited to assist the founders after AlienVault received $8 million in venture capital funding. The company is now targeting midsize enterprises. During 2011, the company implemented UI and deployment packaging improvements. The recently announced Threat Exchange provides automated and anonymized sharing of threat and attack data across the AlienVault installed base. The company will soon release a unified management console that will provide a single configuration and management interface for all security suite components. Development plans include the addition of data analysis functions. The AlienVault Unified SIEM solution should be considered by organizations that need a broad set of integrated security capabilities and by organizations that want a commercially supported product that is based on open source.

Strengths

AlienVault provides integrated SIEM, file integrity monitoring, vulnerability assessment, endpoint control and intrusion detection system capabilities.

Customer references indicate that the software and appliance offerings are much less expensive than corresponding product sets from most competitors in the SIEM space.

Cautions

There is no identity and access management (IAM) integration beyond Active Directory monitoring.

Application integration is primarily with open-source applications.

Return to Top

CorreLog

CorreLog is a small SIEM vendor that provides a Microsoft Windows-based software solution. CorreLog delivers integrated log management and security event management (SEM) functions, and provides basic capabilities in both areas. During the past year, CorreLog has gained some larger customers. ASG, which is its main reseller, has been active in the U.S. and Europe. CorreLog has developed identity obfuscation and work council access interfaces that accommodate some European privacy requirements. During the past year, the vendor has also introduced basic anomaly detection functions, and has improved database monitoring and support for z/OS event sources. Development plans include expansion of anomaly detection capabilities and improvements in the UI.

Strengths

CorreLog has demonstrated a willingness and an ability to rapidly customize its solution for specific use cases.

CorreLog integrates with multiple mainframe security event sources.

We have validated production deployments in the range of 200 to 300 servers and a mix of network devices.

Cautions

CorreLog does not provide event source integration for packaged applications.

It does not provide event source integration for third-party data loss prevention (DLP) or database activity monitoring (DAM) technologies, but there is support for monitoring database activity through native audit functions.

CorreLog is a small vendor and a late entrant in a mature market. It needs to become more visible in competitive evaluations.

Return to Top

eIQnetworks

eIQnetworks targets enterprise security and compliance buyers with its SecureVue product. The company also licenses SEM technology to MSSPs and to network security vendors that use it to build SEM capabilities for their product sets. A distinguishing characteristic of SecureVue is its functional breadth — with capabilities that include SEM, security information management (SIM), security configuration policy compliance, file integrity monitoring, operational performance monitoring functions and some network behavior analysis capabilities. During 2011, the company had success in the U.S. federal segment, positioning its suite as a situational awareness platform capable of security monitoring and security configuration assessment.

During 2011, the company introduced basic behavioral profiling capabilities and reputation database support. Development plans include an expansion of profiling capabilities and an expansion of security configuration assessment functions to compete directly with vendors such as NetIQ and Symantec. SecureVue should be considered by organizations that need a combination of SIEM and security configuration assessment.

Strengths

SecureVue augments SIEM functionality with additional operational performance, as well as asset and configuration policy compliance capabilities. The company has been able to win competitive evaluations against other SIEM vendors, when the customer has a need for capabilities in these adjacent areas.

SecureVue's role-based access and tiered deployment architecture supports federated enterprise and service provider requirements.

Cautions

SecureVue's capabilities are broad in areas that are not part of the typical SIEM problem set.

eIQnetworks is a relatively small vendor with low visibility in competitive evaluations.

Return to Top

HP (ArcSight)

HP ArcSight resides within HP's recently created Enterprise Security Products (ESP) business unit, which also includes HP TippingPoint and HP Fortify. ArcSight Enterprise Security Manager software is oriented to large-scale, SEM-focused deployments. ArcSight Express is an appliance-based offering for Enterprise Security Manager that's designed for the midmarket with preconfigured monitoring and reporting. ArcSight Logger is a line of log management and collector appliances that can be implemented as stand-alone or in combination with Enterprise Security Manager.

During 2011, we have seen the introduction of competitive SIEM technologies within some large ArcSight accounts, with customers indicating a need to expand ArcSight Enterprise Security Manager deployments but citing complexity and cost as inhibitors. During 2011, ArcSight partially addressed these issues for its midsize customers with the release of ArcSight Express version 3, which replaces Oracle Database with a new Correlation Optimized Retention and Retrieval Engine (CORR-Engine) and implements a simplified EPS-based pricing model. ArcSight is expected to provide similar updates to Enterprise Security Manager later this year. In 1Q12, HP released Application Security Monitor, an ArcSight connector implemented on application servers that uses Fortify application assessment capabilities for real-time application security testing. The vendor also announced HP EnterpriseView — a component of HP's Security Intelligence and Risk Management (SIRM) platform, which enables integration with HP and select third-party security technologies. ArcSight Express should be considered for midsize SIEM deployments. ArcSight Enterprise Security Manager is appropriate for larger deployments, as long as sufficient support resources are available.

Strengths

- Enterprise Security Manager provides a complete set of SEM capabilities that can be used to support a security operations center.
- ArcSight Express provides a simplified option for midsize SIEM deployments.
- Optional modules provide advanced support for user activity monitoring, IAM integration and fraud management.
- ArcSight continues to be the most visible vendor in competitive evaluations.

Cautions

- ArcSight Enterprise Security Manager is expensive when compared with competitive solutions at a similar level of scale.
- ArcSight Enterprise Security Manager is complex in terms of deployment and performance management.

Return to Top

IBM (Q1 Labs)

During 4Q11, IBM acquired Q1 Labs and also announced the formation of a security systems division within IBM. The acquisition provides IBM with strong SIEM technology and a replacement for its weak Tivoli SIEM offering. QRadar SIEM appliances provide log management, event management, reporting, and behavioral analysis for networks and applications. QRadar can be deployed as an all-in-one solution for smaller environments, or it can be horizontally scaled in larger environments using specialized event collection, processing and console appliances. A distinguishing characteristic of the technology is the collection and processing of NetFlow data, deep packet inspection (DPI) and behavior analysis for all supported event sources.

Enhancements to QRadar during the past 12 months included indexing and query improvements to support keyword search, and improvements in event storage scalability. Integrations are in progress for IBM DAM, endpoint management, IAM, IPS firewall, as well as governance, risk and compliance (GRC) technologies. Threat intelligence feeds from X-Force will also be released during 2Q12. IBM has announced a co-managed service option for QRadar for customers that want to combine an SIEM technology deployment with monitoring services from IBM.

Strengths

- QRadar provides an integrated view of the threat environment using NetFlow and DPI, in combination with log data from monitored sources.
- Customer feedback indicates that the technology is relatively straightforward to deploy and maintain across a wide range of deployment scales.
- QRadar provides behavior analysis capabilities for both NetFlow and log events.

Cautions

- IBM's execution track record for previous security acquisitions has been inconsistent.
- Because IBM's co-managed offering for QRadar is very new, prospective customers should request customer references from IBM.

Return to Top

LogLogic

In April 2012, Tibco Software acquired LogLogic. This Magic Quadrant evaluation is based on capabilities that were generally available from LogLogic preacquisition. LogLogic provides its core log management appliance line and a number of appliance-based extensions, such as Security Event Manager (real-time monitoring and correlation) and Database Security Manager (DAM and database protection). Virtual appliances are available, and Compliance Manager (compliance dashboards and workflows) is now packaged as a software offering. 2011 updates included a new version of Compliance Manager, the introduction of a virtual appliance and updates to most of the product line. Development plans are focused on the development of behavioral profiling, functions needed by MSSP partners and general improvements in support of cloud environments. LogLogic is a good fit for use cases that are focused primarily on log management or use cases that involve log management and event forwarding to an MSSP or a third-party event manager.

Strengths

The LogLogic line of log management appliances provides competitive log management capabilities that can be integrated with a wide variety of third-party event managers.

It offers on-premises log management and reporting for deployments that also use an MSSP for real-time monitoring.

LogLogic provides the capability to monitor and shield Oracle, SQL Server and Sybase DBMS through the use of specialized agent technology.

Cautions

Typical LogLogic Event Manager implementations continue to be focused on deployments that do not expose LogLogic Event Manager to high event rates. Organizations that require real-time correlation functions at high event rates should require references from LogLogic customers that have deployed at the expected level of scale.

Multiple users report that the event source integration interface is difficult to use.

LogLogic does not provide event source integration for any of the major ERP applications.

Return to Top

LogRhythm

LogRhythm sells its appliance- and software-based SIEM solutions to midsize and large enterprises. The SIEM offering can be deployed in smaller environments with a single appliance or software instance that provides log management and event management, or it can be scaled as a set of specialized appliances or software instances (log management, event management and centralized console). The technology also includes optional agents for major OSs that can be used for filtering at the source. An agent upgrade is available and provides file integrity and system process monitoring for Windows and Unix.

LogRhythm's recent 6.0 release includes performance improvements that the vendor indicates will triple the events per second capacity of existing appliances. Version 6 also includes a new Knowledge Module architecture, which packages reports, investigations, alerts, artificial intelligence engine rules and lists for specific use cases. During 2012, the company plans to introduce statistical analysis improvements and profiling for users and hosts. Development plans include an expansion of behavioral analysis capabilities and the introduction of network behavioral analysis. LogRhythm is a good fit for midsize organizations with limited deployment and support resources that need a mix of log management and event management functions.

Strengths

LogRhythm provides a balance of log management, reporting, event management, privileged user, and file integrity monitoring to support security operations and compliance use cases.

Its appliance format and configuration wizards allow for fast deployment with minimal resources.

The company's quarterly health check program gets high marks from customers that value the continuing engagement to encourage momentum with security monitoring.

LogRhythm has added resources in sales, channel and professional services to address enterprise market requirements. As a result, it has doubled its inclusion on Gartner client shortlists during 2011 compared with 2010.

Cautions

LogRhythm is still small enough to be an easy acquisition by large vendors that want to enter the SIEM market.

Event correlation capabilities are optimized for the most common use cases but are not as advanced as technologies that lead in these areas.

Return to Top

McAfee (NitroSecurity)

McAfee entered the SIEM market with the 4Q11 acquisition of NitroSecurity. McAfee is gradually integrating and rationalizing the NitroSecurity technology with its portfolio of security technologies. The McAfee Enterprise Security Manager (formerly NitroView) line of appliances combines SIM and SEM functions with in-line network monitors, which implement DPI to obtain data and application context and content for security events. In addition, McAfee Enterprise Security Manager provides integrated DAM technology. During 2011, NitroSecurity released its Advanced Correlation Engine, which augments rule-based correlation with risk-based activity profiling.

McAfee has carried forward elements of the former NitroView network monitoring technology that support critical infrastructure use cases, and the DAM and application and data monitoring (ADM) functions. During 2Q12, McAfee will release Enterprise Security Manager version 9.1, which includes the integration of threat intelligence from McAfee Global Threat Intelligence, risk data from McAfee Risk Advisor, and asset data from McAfee Vulnerability Manager and McAfee ePolicy Orchestrator. McAfee Enterprise Security Manager is a good choice for organizations that require high-performance analytics under high-event-rate conditions.

Strengths

Customer references have validated very high scalability and query performance levels for the McAfee Enterprise Security Manager event data store.

The McAfee Enterprise Security Manager ADM component provides application and data access monitoring from network-based packet inspection, which augments log-based monitoring.

Cautions

- Potential customers of the ADM component should evaluate their network architecture to determine the required number and availability of monitoring points.
- McAfee does not have a track record for supporting a technology whose primary value is integration with third-party event sources.

Return to Top

NetIQ (Novell)

During 2Q11, NetIQ announced the addition of the complete portfolio of Novell identity and security solutions, as well as select Novell data center solutions, to its solution portfolio. Sentinel, Sentinel Log Manager and Compliance Management Platform have been added to NetIQ's security monitoring portfolio, which includes Security Manager and the Change Guardian product set. NetIQ and Novell security monitoring technologies are largely synergistic, but realization of value by customers required investment and execution by NetIQ.

Sentinel is very strong in real-time event management and correlation for the network security use case. Security Manager support for this use case has been weak. Security Manager has host- and agent-based monitoring capabilities for server platforms and Microsoft Active Directory, which most SIEM technologies (including Sentinel) lack.

During 4Q11, NetIQ released Sentinel 7, which eliminates the requirement for a relational database for event storage, and provides simpler deployment through virtual appliance packaging, improved reporting and UI improvements. During 1Q11, the vendor added an integration with Security Manager (for existing customers) and a lightweight integration with Change Guardian and host agent infrastructure.

Strengths

- Sentinel and Sentinel Log Manager are appropriate for large-scale, SEM-focused deployments.
- The Change Guardian product line provides agent-based monitoring and change detection for Active Directory and Windows, and file integrity monitoring for host systems.
- NetIQ agent technology can provide an alternative to native platform audit functions for use cases that require user and data access monitoring for servers.

Cautions

- NetIQ needs to complete the rationalization of its two security monitoring technologies by providing a unified administrative interface.
- NetIQ lacks visibility into competitive evaluations of security monitoring technology.

Return to Top

Prism Microsystems

Prism Microsystems' EventTracker is SIEM software that is targeted primarily at midsize commercial enterprises and government organizations with security and operations event management and compliance reporting requirements. EventTracker can be deployed in a virtual environment. The EventTracker agent provides support for file integrity monitoring and USB control. Basic profiling capabilities are provided via a behavior module that can establish a baseline of a user-configurable period of time and can issue alerts on deviations from normal. 2011 updates included StatusTracker (autodiscovery and availability monitor), a data mart to support historical analysis and a managed SIEM offering. Development plans include a built-in trouble-ticketing system, support for Amazon Relational Database Service and ongoing additions of knowledge packs for log sources. EventTracker is suited for midsize businesses that require log management, SEM, compliance reporting and operations monitoring via a software-based solution.

Strengths

- EventTracker is easy to deploy and maintain, with compliance and use-case-specific knowledge packs that provide prebuilt alerts, correlation rules and reports.
- EventTracker's Web interface supports role-based access to support security, compliance and operations use cases, and EventTracker supports centralized agent deployment and management in Windows environments.

Cautions

- EventTracker's capabilities for application monitoring and integration with IAM products are more limited than other SIEM products targeting enterprise deployments.
- The company lacks visibility in the midsize market compared with other SIEM vendors that are aggressively targeting this space.

Return to Top

RSA (EMC)

RSA, The Security Division of EMC, provides an SIEM solution that is composed of two components — enVision provides SEM, SIM and log management; and NetWitness provides more advanced security analytics. RSA (EMC) has one of the largest SIEM installed bases; however, during 2011, enVision continued to be the most frequently displaced SIEM technology, primarily due to ad hoc query and report performance issues. The issue is most severe in larger enVision deployments. Late in 2011, RSA (EMC) released enVision 4.1, which contains scalability and query performance improvements, but does not completely resolve the issue. The company has recently announced NetWitness for Logs, a data input feature of NetWitness v.9.7 that enables ingestion and analysis of log data sources. NetWitness can accept nonparsed data from enVision and can also collect logs on its own. NetWitness analytics and reporting can provide relief to the performance issues suffered by large enVision customers. However, NetWitness does not yet have cross-data-source correlation capabilities that would enable it as a general SIEM solution, so enVision is still needed.

RSA plans to carry both the enVision and NetWitness technologies for the near term, but development and sales focus for security use cases will move to the NetWitness platform, as the company further develops real-time monitoring capabilities and packaging options for the midmarket. RSA plans to introduce a single UI that can be used across enVision and NetWitness. For smaller deployments, RSA continues to recommend enVision to its customers. For larger deployments, RSA is positioning NetWitness for Logs, in combination with enVision, when cross-data-source correlation is needed. NetWitness for Logs should be considered by organizations that have deployed enVision and need to overcome query and reporting performance limitations.

Strengths

NetWitness for Logs provides high-performance analytics of security log event data that can be integrated with full-packet capture data.

RSA has integrated its SIEM, network forensics, DLP and GRC technologies.

Cautions

enVision customers frequently complain of query performance issues as the size of the back store grows and should evaluate the addition of NetWitness for Logs.

Until RSA develops NetWitness event correlation capabilities, larger organizations that need to implement security monitoring technology that includes event correlation in the short term should also consider alternatives from other vendors.

As RSA's SIEM technology enters a period of transition, midsize organizations that are evaluating enVision should also consider alternatives from other vendors.

Return to Top

S21sec

S21sec is a security company based in Spain that provides a cyberintelligence service and the Bitacora SIEM solution, which incorporates its endpoint cyberintelligence agent. Geographically, the largest installed bases are in Europe (Spain) and Latin America (Brazil, Mexico and Panama); however, S21sec is also becoming active in projects in the Middle East and Africa. Industry verticals include financial services, as well as those that require operational control system monitoring. The endpoint security technology is an agent that can implement endpoint control and discover malware, such as keyloggers and rootkits. Windows, Linux and Mac OS X systems are supported. The company is working on developing an anomaly detection engine.

Strengths

S21sec provides a combination of SIEM, endpoint security and security intelligence functions.

Bitacora should be considered by companies that want to acquire an SIEM solution from a vendor that is oriented toward Spain or Spanish-speaking customers.

S21sec should also be considered by organizations that need endpoint malware detection, forensics and cyberintelligence capabilities to support fraud detection use cases.

Cautions

Organizations that are considering Bitacora should ensure that there is a good match with respect to S21sec's regional presence.

S21sec is beginning to develop a sales presence in North America, but technical support is located in Spain.

Bitacora lacks support for major packaged applications such as SAP and PeopleSoft.

We have only been able to validate midsize deployments, although the vendor indicates that large-scale deployments exist.

Return to Top

Sensage

The Sensage solution is optimized for precision analytics and compliance reporting for a large event data store, and the company has successfully pursued large deployments that require this capability. Sensage continues to pursue large deals for specific use cases within such verticals as U.S. and European federal governments, large telcos and financial services, using a combination of direct and partner sales. Sensage has also successfully pursued use cases that require application layer and/or user-oriented monitoring. 2011 updates included the release of Open Access Extension, an interface to the event data warehouse that allows third-party business intelligence tools or custom applications to access/analyze the stored data using standard interfaces. Development plans include a redesign of the UI.

Strengths

Sensage is optimized for organizations that require high-volume event collection, monitoring, analytics and reporting for large amounts of log data over long periods for audit, compliance and internal investigations.

The company has explicit support for SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and other packaged application providers. Its technology supports the precise analytics needed for use cases, such as fraud detection.

Sensage is a good fit for use cases that require compliance reporting or security analytics for a large event store with basic real-time monitoring requirements.

Cautions

Organizations that require only basic log management functions should consider simpler and less expensive offerings that focus on collection and basic reporting.

Although the company has just introduced Sensage Swift, a rapid deployment option, it was not evaluated for this Magic Quadrant, and customer feedback during the evaluation period continued to indicate that the enterprise version of Sensage is complex to deploy and maintain.

Sensage's technology is not widely deployed for use cases that are focused on SEM. Although some customers have deployed real-time monitoring for all event sources, most customers continue to implement a combination of real-time and short-cycle monitoring, and there is no native incident management capability.

Sales, marketing and technology "packaging" is oriented toward larger environments that require large-scale security analytics — a specific use that is not at the center of the market.

Return to Top

SolarWinds

SolarWinds entered the SIEM market with the 3Q11 acquisition of TriGeo. The company repackaged TriGeo's appliance and now sells SolarWinds Log and Event Manager software as a virtual appliance. Immediately after the acquisition, SolarWinds focused its sales attention solely on its core buying center — the IT operations area. We initially had concerns about the company's long-term commitment to the application of the technology for security use cases. SolarWinds has since engaged the security buying center, and will continue to enhance the technology for security use cases. The vendor also plans integrations with its operations monitoring technologies to support use cases such as change detection and failure root cause analysis. Development plans include an expansion of integrations with the SolarWinds portfolio of network and systems monitoring products. The company is also exploring partnerships with other security product/technology vendors.

Strengths

SolarWinds Log and Event Manager is a good fit for small and midsize companies that require SIEM technology that is easy to deploy.

The technology is also well-suited for organizations that have already invested in other SolarWinds technology solutions.

Cautions

The technology is optimized for small-to-midsize deployments, and other SIEM solutions are a better fit for large-scale deployments.

The technology and its associated deployment services are not designed for use cases that require extensive customization and integration with other IT management technologies.

Return to Top

Splunk

Splunk is widely deployed by IT operations and application support teams for log management analytics, monitoring and advanced search. Within security, we have historically seen Splunk deployed to provide converged security and operations log management functions or to augment SIEM deployments. However, during the past 18 months, there has been an expansion of customers deploying the Splunk App for Enterprise Security for stand-alone SIEM use cases. Splunk provides real-time correlation and alerting. The Splunk App for Enterprise Security provides predefined searches, reports, dashboards, visualization and real-time monitoring to support security monitoring and compliance reporting use cases. Splunk can also be used for file integrity monitoring. Development plans include the creation of profiling and anomaly detection capabilities.

Strengths

Splunk provides highly flexible analytics for large amounts of data and has successfully been adapted for a wide variety of use cases.

Splunk is often deployed by IT operations and application support teams as log management analytics infrastructure. It can also be used as the log management infrastructure for IT security and supports the convergence of IT operations, application intelligence and IT security silos.

Use cases that require analysis of a large number of data sources that are not formally supported by other SIEM vendors (for example, an organization's in-house-developed application portfolio) are ideal for Splunk's approach of normalization at the time of event data access.

Cautions

Splunk App for Enterprise Security requires significant customization. It is not a good fit for security organizations that lack the requisite staffing and expertise.

While Splunk App for Enterprise Security provides productized parsing support for Oracle common audit logs, it lacks productized support for other database management systems and DLP technologies. The user can obtain predefined maps for many of these sources from Splunk's community-supported Splunkbase.

Splunk does not have predefined parsing support for IAM infrastructure, beyond the use of the Windows Management Instrumentation interface for Active Directory. The user must build his or her own keyword searches for these sources; however, predefined parsing is not required for collection.

Return to Top

Symantec

Symantec Security Information Manager (SSIM) is delivered as an appliance, and provides SIM and SEM capabilities. Symantec has integrated SSIM with its Security Endpoint Protection (SEP); IT governance, risk and compliance management (GRCM); and DLP technologies. In addition, SSIM is dynamically updated with threat and vulnerability data content from Symantec's DeepSight security research and managed security area. During the past 12 months, Symantec released a new line of SIEM appliances, released minor functional and usability enhancements, and introduced support for 15 new event sources. Development plans are focused on incident management improvements and enhanced support for cloud environments.

Strengths

Symantec SIEM covers all major core SIEM capabilities, and we have been able to validate successful large deployments.

Symantec has integrated a DeepSight threat intelligence feed with SSIM and is ahead of competitors in this area.

Cautions

The company has not been very visible in the competitive evaluations of SIEM technology that we have seen from Gartner clients.

During the past few years, Symantec has not invested in the development of this technology to the same degree as its leading competitors, and some customers complain about a lack of new capabilities in areas such as IAM integration, log routing and keyword search.

We have feedback from clients that Symantec has been slow to provide enhancements to the integration between its MSSP service and SIEM offering, and that the use of SSIM in a co-managed deployment is sometimes discouraged.

Existing SSIM customers that need deployment support for use cases beyond initial deployment have indicated that services are sometimes difficult to obtain from Symantec and its service provider partners.

The technology is not a good fit for implementations that require integration with specific IAM technologies beyond the narrow set of directory and network authentication technologies currently supported.

Return to Top

Tango/04

Tango/04 Visual Message Center provides operational event correlation, business process monitoring and SIEM solutions. Tango/04 is typically used by midsize financial institutions in Europe and Latin America (where the company is called Barcelona/04 because of trademark issues with the Tango name there). The company indicates that half its customers use the technology for IT operations and IT security use cases. The technology can parse event data from major OSs, network devices, vulnerability assessment programs and endpoint security programs. Updates during the past 12 months include the introduction of a configuration assessment module for Windows and a multiplatform agent (Unix, Linux and Windows) for the execution of remote commands and remote scripts. The company is also expanding the UI to support tablet devices.

Strengths

The technology is a good fit for midsize companies within the geographic span of Tango/04 that want to use a common event monitoring technology for IT security and IT operations use cases.

Data-monitoring capabilities include file integrity monitoring, database monitoring via standard audit logs, and modules that provide transaction-level monitoring for SQL Server and iSeries.

The technology has been applied by many customers for application activity monitoring.

Cautions

The primary orientation of the technology is for IT operations use cases, such as availability and performance monitoring.

Its IAM integration is limited to Active Directory.

Its security device support is very narrow compared with the majority of established SIEM vendors.

Tango/04 does not have a sales and support presence in North America, and there is a general lack of visibility in competitive evaluations of SIEM technologies.

Return to Top

Tenable Network Security

Tenable Network Security's SIEM software solution includes the SecurityCenter console and the Log Correlation Engine (LCE). LCE provides log and event collection, analysis and reporting. SecurityCenter adds the ability to correlate events with data from Tenable's Nessus vulnerability scanner and Passive Vulnerability Scanner (PVS) to provide unified asset discovery, vulnerability detection, event management log collection and reporting. Windows and Unix log collection agents can also provide file integrity and change monitoring. Tenable's SIEM customers tend to use the vulnerability scanning and configuration assessment capabilities as components of their SIEM deployments.

SecurityCenter, Nessus and PVS can be deployed as software, or as physical or virtual appliances. The LCE is available as software. SecurityCenter includes basic NetFlow monitoring capabilities. PVS can monitor selected network traffic, such as file downloads, and generate alerts in SecurityCenter. During 2011, Tenable introduced daily threat list updates for external threat detection and query response time improvements. LCE 4.0 will include full text indexing and search support, higher compression rates, centralized agent management and load-balanced log processing. The technology is a good fit for organizations that want unified management and reporting for vulnerability assessment and SIEM functions.

Strengths

Customers cite the integration of SecurityCenter and LCE with Nessus and PVS as a strength for SIEM deployment, and the combination of capabilities results in strong coverage of PCI and the Federal Information Security Management Act (FISMA) compliance requirements.

SecurityCenter and LCE offer broad coverage of network-based security technologies, including DLP, firewalls, and intrusion detection and prevention products.

The SecurityCenter UI provides improved access to the product's searching, filtering, reporting and dashboard functions.

Tenable has added management resources for service, including support and training, as well as for finance and marketing. Customers report strong satisfaction with Tenable's technical support.

Cautions

LCE lacks log routing functions (forwarding a filtered subset of log data in native format) that could be used to integrate with a third-party event manager.

LCE lacks integration with IAM policy sources, but is able to extract user identity information from logs.

LCE lacks support for major packaged applications.

SecurityCenter lacks the degree of workflow integration with corporate ticketing and directories found in competitive enterprise SIEM products, although SecurityCenter has an internal ticketing capability and can initiate tickets by email to corporate ticketing systems.

Return to Top

Tier-3

Tier-3 is a small Australia-based company that provides SIEM technology primarily to the Asia/Pacific region and the U.K. The company has established offices in London and is increasing its sales focus on Europe. The company's Huntsman SIEM software is composed of three modules. Huntsman Log Analyzer provides log management and reporting. Huntsman Data Protector provides real-time monitoring and rule-based correlation. Huntsman Protector 360 provides behavioral anomaly detection. Updates released in 2011 include multitenant support and workflow enhancements that are directed at MSSP customers. The company plans to release virtual appliance packaging. Reference account discussions have validated that the technology is a good fit for midsize deployments that are oriented primarily to threat detection and security monitoring.

Strengths

We have validated successful customer deployments that use Huntsman for anomaly detection and profiling of user activity and resource access.

Customers report that only a modest tuning effort is needed to make anomaly detection and profiling operationally effective.

Cautions

Organizations that are considering Huntsman should ensure that there is a good match with respect to Tier-3's regional presence.

Huntsman uses a commercial relational database for parsed events, and users will need database administration and performance management skills to support the deployment.

IAM integration is limited to Active Directory and a narrow set of network authentication sources.

Return to Top

Trustwave

Trustwave is primarily a security service provider that delivers PCI assessment services, vulnerability assessment services, managed security services and security consulting; however, it has also built a security product portfolio through the acquisition of Secure Web Gateway, DLP, Web application firewall, network access control and encryption technologies. The SIEM technology is composed of two components — the Trustwave SIEM Operations Edition (SIEM OE) software, and the Trustwave SIEM appliance. Trustwave SIEM OE is highly customizable and optimal for large-scale, SEM-focused deployments. Trustwave will sell this to its large customers, and it has instrumented its own security operations center with the technology. Trustwave SIEM is a customer-managed appliance that provides data collection, log management and basic SEM for midsize deployments. Trustwave Managed SIEM is a version of the appliance that provides on-premises log collection and event forwarding for Trustwave's Managed SIEM service. During 2011, Trustwave released an upgraded MSSP portal, upgraded the appliance (v.1.2.1) and upgraded the OE software to v.5.9, which included improved dashboarding. The appliance now supports granular selective event forwarding to OE.

Strengths

Trustwave offers a wide choice of SIEM sourcing options, and should be considered by customers that want a mix of SIEM managed services and self-managed technologies, or the ability to move from one sourcing option to another.

SIEM OE is a good fit for large-scale, SEM-focused deployments in which a high degree of customization is required and capable support resources are available.

Trustwave SIEM is suitable for midsize and distributed environments that require configurable predefined functions and simplified deployments.

Support for the threat management use case includes threat intelligence from iDefense, as well as anomaly detection and proofing capabilities.

Cautions

Potential buyers and current users that are interested in mixing deployment modes (products and managed services) will need to carefully track Trustwave's progress in integrating the various product and service options, and in providing unified administration and functional capabilities.

Trustwave has a diverse software portfolio to manage in addition to its core security service business. Although Trustwave has released enhancements to SIEM (appliance, managed and OE versions) during 2010 and 2011, the 2012 release of version 6 marks the first major update to OE during the past two years.

Trustwave is not visible in competitive evaluations of SIEM technology.

Return to Top

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Return to Top

Added

IBM's acquisition of Q1 Labs has closed, and the designation on the SIEM Magic Quadrant is now IBM (Q1 Labs).

McAfee's acquisition of NitroSecurity has closed, and the designation on the SIEM Magic Quadrant is now McAfee (NitroSecurity).

NetIQ's acquisition of Novell's security technology has closed, and the designation for the NetIQ and Novell technologies on the SIEM Magic Quadrant is now NetIQ (Novell).

SolarWinds acquired TriGeo.

Return to Top

Dropped

Quest Software was dropped from the Magic Quadrant because its technology is increasingly focused on server monitoring and is too narrowly focused to solve threat management use cases.

Tripwire was dropped because of a change in product strategy that focuses on integration with third-party SIEM technologies to provide system configuration and change context. Tripwire Log Center will be focused on augmenting Tripwire capabilities to provide greater system-state intelligence.

netForensics was dropped because of its increasing focus on MSSPs as its primary customer (versus corporate security organizations).

Return to Top

Inclusion and Exclusion Criteria

These criteria had to have been met for vendors to be included in the 2012 SIEM Magic Quadrant:

The product must provide SIM and SEM capabilities.

The product must support data capture from heterogeneous data sources, including network devices, security devices, security programs and servers.

The vendor must appear on the SIEM product evaluation lists of end-user organizations.

The solution must be delivered to the customer environment as a software- or appliance-based product (not a service).

Vendors were excluded if:

They provide SIEM functions that are oriented primarily to data from their own products.

They position their products as an SIEM offering, but the products do not appear in the competitive shortlists of end-user organizations.

They had less than $4 million in SIEM product revenue during 2011.

The solution is delivered exclusively as a managed service.

Return to Top

Evaluation Criteria

Ability to Execute

Product/service evaluates the vendor's ability and track record to provide product functions in areas such as log management, compliance reporting, SEM and deployment simplicity.

Overall viability includes an assessment of the organization's financial health, the financial and practical success of the overall company, and the likelihood that the business unit will continue to invest in the SIEM technology segment.

Sales execution/pricing evaluates the technology provider's success in the SIEM market and its capabilities in presales activities. This includes SIEM revenue and the installed base size, growth rates for SIEM revenue and the installed base, presales support, and the overall effectiveness of the sales channel. The level of interest from Gartner clients is also considered.

Market responsiveness and track record evaluates the match of the SIEM offering to the functional requirements stated by buyers at acquisition time, and the vendor's track record in delivering new functions when they are needed by the market. Also considered is how the vendor differentiates its offerings from those of its major competitors.

Marketing execution evaluates the SIEM marketing message against our understanding of customer needs, and also evaluates any variations by industry vertical or geographic segments.

Customer experience is an evaluation of product function or service within production environments. The evaluation includes ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed by conducting qualitative interviews of vendor-provided reference customers in combination with feedback from Gartner clients that are using or have completed competitive evaluations of the SIEM offering.

Operations is an evaluation of the organization's service, support and sales capabilities, and includes an evaluation of these capabilities across multiple geographies.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	High
Market Responsiveness and Track Record	High
Marketing Execution	Standard
Customer Experience	High
Operations	High

Source: Gartner (May 2012)

Completeness of Vision

Market understanding evaluates the ability of the technology provider to understand buyer needs and to translate those needs into products and services. SIEM vendors that show the highest degree of market understanding are adapting to customer requirements in areas such as log management, simplified implementation and support, and compliance reporting, while also meeting SEM requirements.

Marketing strategy evaluates the vendor's ability to effectively communicate the value and competitive differentiation of its SIEM offering.

Sales strategy evaluates the vendor's use of direct and indirect sales, marketing, service, and communications affiliates to extend the scope and depth of market reach.

Offering (product) strategy is the vendor's approach to product development and delivery that emphasizes functionality and feature sets as they map to current requirements for SIM and SEM. Development plans during the next 12 to 18 months are also evaluated.

Because the SIEM market is mature, there is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and consolidated administration capabilities. In this evaluation, we neutralized relative ratings of vendors with capabilities in these areas, but there is a severe "vision" penalty for the few vendors that continue to have shortcomings in this area.

In this year's SIEM vendor evaluation, we place greater weight on current capabilities that aid in targeted attack detection:

Vendor capabilities and plans for profiling and anomaly detection to complement existing rule-based correlation

Threat intelligence

User activity monitoring capabilities, which include monitoring of administrative policy changes and integration with IAM technologies, for automated import of access policy (user context) for use in monitoring

Data access monitoring capabilities, which are composed of DAM (direct monitoring of database logs and integration with DAM products), DLP integration, and file integrity monitoring (native capability and integration with third-party products)

Application layer monitoring capabilities includes integration with third-party applications (for example, ERP financial and HR applications, and industry vertical applications), for the purpose of user activity and transaction monitoring at that layer; the external event source integration interface that is used to define the log format of an organization's in-house-developed applications; and the ability to derive application context from external sources

Large SIEM vendors are focused on integration with related asset management, security assessment, and shielding technologies within their own security and operations technology portfolios. Despite the vendor focus on expansion of capability, we continue to heavily weight deployment simplicity. Users still value this attribute over breadth of coverage beyond the core use cases. There is a danger of SIEM products (which are already complex) becoming too complex as vendors extend capabilities. Vendors that are able to provide deployment simplicity as they add function will be the most successful in the market.

We added an evaluation of hybrid or co-managed options, because a growing number of clients are asking about the possibility of limited monitoring services for their SIEM technology deployments.

Business model evaluates the vendor's underlying business proposition but is not rated in this evaluation.

Vertical industry strategy evaluates vendor strategies to support SIEM requirements that are specific to industry verticals.

Innovation evaluates the vendor's development and delivery of SIEM technology that is differentiated from the competition in a way that uniquely meets critical customer requirements. Product capabilities and customer use in areas such as application layer monitoring, fraud detection and identity-oriented monitoring are evaluated, in addition to other capabilities that are product-specific and are needed and deployed by customers.

There is a strong weighting of capabilities that are needed for security monitoring and targeted attack discovery — user and data access monitoring, application activity monitoring, ad hoc query and analytics, capabilities/plans for profiling and anomaly detection, and threat intelligence.
We added an evaluation of technology capabilities/vendor plans for monitoring cloud workloads.

Geographic strategy — Although the SIEM market is centered in North America, there is growing demand for SIEM technology in Europe and Asia/Pacific, driven by a combination of compliance and threat management requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for these geographies.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	No Rating
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (May 2012)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a good functional match to general market requirements, have been the most successful in building an installed base and revenue stream within the SIEM market, and have a relatively high viability rating (because of SIEM revenue, or SIEM revenue in combination with revenue from other sources). In addition to providing a technology that is a good match to current customer requirements, Leaders also show evidence of superior vision and execution for anticipated requirements. Leaders typically have relatively high market share and/or strong revenue growth, and have demonstrated positive customer feedback for effective SIEM capabilities and related service and support.

Return to Top

Challengers

The Challengers quadrant is composed of vendors that have a large revenue stream (typically because the vendor has multiple product and/or service lines), at least a modest-size SIEM customer base and products that meet a subset of the general market requirements. Many of the larger vendors in the Challengers quadrant position their SIEM solutions as an extension of related security and operations technologies. Companies in this quadrant typically have strong execution capabilities, as evidenced by financial resources, a significant sales and brand presence garnered from the company as a whole, or other factors. However, Challengers have not demonstrated as rich a capability or track record for their SIEM technologies as vendors in the Leaders quadrant have.

Return to Top

Visionaries

The Visionaries quadrant is composed of vendors that provide products that are a good functional match to general SIEM market requirements, but have a lower Ability to Execute rating than the Leaders. This lower rating is typically because of a smaller presence in the SIEM market than the Leaders, as measured by installed base or revenue size or growth, or by smaller overall company size or general viability.

Return to Top

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors that are regional in focus, or provide SIEM technology that is a good match to a specific SIEM use case, a subset of SIEM market requirements. Niche Players focus on a particular segment of the client base or a more-limited product set. Their ability to outperform or innovate may be affected by this narrow focus. Vendors in this quadrant may have a small or declining installed base, or be limited, according to Gartner's criteria, by a number of factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broader set of capabilities to enterprises now and during the 12-month planning horizon. Inclusion in this quadrant does not reflect negatively on the vendor's value in the more narrowly focused service spectrum.

Return to Top

Context

SIEM technology provides:

- SIM — log management and compliance reporting
- SEM — real-time monitoring and incident management for security-related events from networks, security devices, systems, and applications

SIEM technology is typically deployed to support three primary use cases:

- Threat management — real-time monitoring and reporting of user activity, data access, and application activity in combination with effective ad hoc query capabilities
- Compliance — log management and compliance reporting
- A deployment that provides a mix of threat management and compliance capabilities

Although many SIEM deployments have been funded to address regulatory compliance reporting requirements, the rise in successful targeted attacks has caused a growing number of organizations to use SIEM for threat management to improve security monitoring and early breach detection. The SIEM market is composed of technology providers that support all three use cases; however, there are variations in the relative level of capability for each use case, in deployment and support complexity, in the scope of related functions that are also provided, and in product support for capabilities related to targeted attack detection (such as user activity monitoring, data access monitoring, application activity monitoring, the use of threat intelligence and anomaly detection). This year's evaluation more heavily weights capabilities that support targeted attack detection. As a companion to this research, we evaluate the SIEM technologies of 12 vendors with respect to the three major use cases.[1]

Organizations should consider SIEM products from vendors in every quadrant of this Magic Quadrant based on their specific functional and operational requirements. Product selection decisions should be driven by organization-specific requirements in areas such as the relative importance of compliance and threat management; the scale of the deployment; SIEM product deployment and support complexity; the IT organization's project deployment and technology support capabilities; identity, data and application monitoring requirements; and integration with established applications, data monitoring and identity management infrastructure.[2]

Security managers considering SIEM deployments should first define the requirements for SEM and reporting. The requirements definition effort should include capabilities that will be needed for subsequent deployment phases. The project will benefit from the input of other groups, including audit/compliance, identity administration, IT operations and application owners (see "How to Deploy SIEM Technology"). Organizations should also describe their network and system deployment topology, and assess event rates, so that prospective SIEM vendors can propose solutions to company-specific deployment scenarios. The requirements definition effort should include phase deployments beyond the initial use case. This Magic Quadrant evaluates technology providers with respect to the most common technology selection scenario — an SIEM project that is funded to satisfy a combination of threat monitoring/response and compliance-reporting requirements.

Return to Top

Market Overview

During the past year, demand for SIEM technology has remained strong. During this period, the number of Gartner inquiry calls from end-user clients with funded SIEM projects matched levels of the previous 12 months,[3] and most vendors have reported increases in customers and revenue.[4] During 2011, the SIEM market grew from $987 million to $1.1 billion, achieving a growth rate of 15%. In North America, there continues to be many new deployments by smaller companies that need log management and compliance reporting. There are also new deployments by larger companies that are conservative adopters of technology. Both of these customer segments place high value on deployment and operational support simplicity. Some large companies are also re-evaluating SIEM vendors to replace SIEM technology associated with partial, marginal or failed deployments. During this period, there has been a stronger focus on security-driven use cases from new and existing customers. There is growing demand for SIEM technology in Europe and Asia/Pacific, driven by a combination of compliance and threat management requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for these geographies.

The SIEM market is mature and very competitive. We are in a broad adoption phase, in which multiple vendors can meet the basic log management, compliance and event monitoring requirements of a typical customer. The greatest area of unmet need is effective targeted attack and breach detection. Organizations are failing at early breach detection, with more than 85% of breaches undetected by the breached organization.[5] The situation can be improved with better threat intelligence, the addition of behavior profiling and better analytics. Most companies expand their initial SIEM deployments over a three-year period to include more event sources and greater use of real-time monitoring. SIEM vendors have large existing customer bases, and there is an increasing focus on selling more SIEM technology into existing accounts. Several SIEM vendors are beginning to position their technologies as "platforms" that can provide security, operations and application analytics.

SIEM Vendor Landscape

Twenty vendors met Gartner's inclusion requirements for the 2012 SIEM Magic Quadrant. Twelve are point solution vendors, and eight are vendors that sell additional security or operations products and services. There were four notable acquisitions in the SIEM market during the past 12 months. IBM acquired Q1 Labs to gain strong technology as a replacement of its Tivoli SIEM offering. McAfee entered the SIEM market with the acquisition of NitroSecurity. NetIQ acquired Novell's security monitoring technology. SolarWinds entered the SIEM market with its acquisition of TriGeo. In addition, as we were completing the research process, Tibco Software announced its intention to acquire LogLogic. Because SIEM technology is now deployed by a broad set of enterprises, vendors are responding with a shift in sales and product strategies. SIEM vendors are increasingly focused on covering additional use cases, so that they can continue to sell additional capabilities to their customer bases. Some SIEM technology purchase decisions do not include a competitive evaluation, because the technology is sold by a large vendor in combination with related security, network or operations management technologies. Many SIEM vendors are developing sales channels that can reach the midsize market in North America. Sales effectiveness in Europe and Asia/Pacific is becoming increasingly important as SIEM deployments increase in these regions.

Some large vendors (HP and IBM) are positioning SIEM as a platform that can unify adjacent security and operations technologies within their portfolios. A number of large vendors have always provided (Symantec) or have recently released (IBM, HP, McAfee and RSA) an integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (HP, IBM and Symantec) are marketing the idea of co-managed SIEM technology deployments that include varying levels of monitoring services. RSA (EMC) is executing a strategy to provide a common platform (NetWitness) for log management and packet capture, and to also integrate with its GRC platform. Symantec sells SIEM to large enterprises that use its endpoint security products, and has integrated its SIEM and IT GRCM offerings.

Several vendors are not included in the Magic Quadrant because of a specific vertical market focus and/or SIEM revenue levels:

- AccelOps is a small and recent entrant to the SIEM market that does not meet inclusion revenue thresholds. The vendor provides security and operations monitoring via a unified log management and event management infrastructure with domain-specific views and analytics.
- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer.
- netForensics focuses on MSSPs as its primary customer (versus corporate security organizations).
- Quest Software's monitoring technology is primarily focused on server monitoring.
- Tripwire's Log Center is focused on augmenting Tripwire capabilities to provide greater system state intelligence.

A few vendors sell solutions that are based on licensed SIEM technology. Q1 Labs licenses its technology to vendors (Juniper Networks and Enterasys) that implement its technology on their own appliances, and add specific integrations with their respective management infrastructures. Sensage licenses its SIEM technology to Cerner, which has integrated it with its packaged healthcare applications for application activity monitoring and audit.

Customer Requirements — Security Monitoring and Compliance Reporting for Systems, Users, Data and Applications

While the primary source of funding for SIEM deployments continues to be regulatory compliance, security use cases are ascending in relative importance. Even when the initial SIEM deployment is funded to close a compliance gap, the IT security organization owns the project, and there is a strong motivation to improve security monitoring capabilities. The number of new European and Asia/Pacific SIEM deployments has been rising, and the initial focus (security monitoring or compliance) varies by region. Adoption of SIEM technology by a broad set of companies has fostered demand for products that provide predefined compliance reporting and security monitoring functions, as well as ease of deployment and support. Log management functions have become an expected and standard component of an SIEM technology architecture.

SIEM solutions should:

- Support the real-time collection and analysis of events from host systems, security devices and network devices, combined with contextual information for users, assets and data.
- Provide long-term event and context data storage and analytics.
- Provide predefined functions that can be lightly customized to meet company-specific requirements.
- Be as easy as possible to deploy and maintain.

The security organization often wants to employ SIEM to improve capabilities for external and internal threat discovery and incident management (see "Using SIEM for Targeted Attack Detection"). As a consequence, there are requirements for user activity and resource access monitoring for host systems and applications (see "Effective Security Monitoring Requires Context"). In this year's SIEM vendor evaluation, we have placed greater weight on capabilities that aid in targeted attack detection, including support for data access, user activity, application activity monitoring, profiling and anomaly detection, threat intelligence, and effective analytics.

Scalability

Scalability is a major consideration with SIEM deployments. For an SIEM technology to meet the requirements for a given deployment, it must be able to collect, process, store and analyze all security relevant events. Events that need to be monitored in real time have to be collected and processed in real time. Event processing includes parsing, filtering, aggregation, correlation, alerting, display, indexing and writing to the back store. Scalability also includes access to the data for analytics and reporting — even during peak event periods — with ad hoc query response times that do not preclude the use of an iterative approach for incident investigation. Query performance needs to hold up, even as the event store grows over time. We characterize the size of a deployment based on three principal factors:

- The number of event sources
- The sustained events per second (collected after filtering, if any)
- The size of the event back store

We assume a mix of event sources that are dominated by servers but also include firewalls, intrusion detection sensors and network devices. Some deployments also include a large number of PC endpoints, but these are not typical, and PC endpoint counts are not included in our totals. The boundaries for small, midsize and large deployments are not absolute, because some deployments may have a large number of relatively quiet event sources, while others will have a smaller number of very busy event sources. For example, a deployment with several busy log sources may exceed the EPS limits set below for a small deployment, but will still be small architecturally.

We define a small deployment as one with 200 or fewer event sources, a sustained EPS rate of 400 events per second or less, and a back store sized at 800GB or less. A large deployment is defined as one with more than 750 event sources, a sustained event rate of more than 5,000 events per second, and a back store of 10TB or more. Midsize deployments fall between the boundaries of small and large deployments. There are also some very large deployments that have high thousands of event sources, sustained event rates of more than 25,000 EPS, and a back store of more than 50TB. We may indicate that a vendor's SIEM technology is ideally suited for a small, midsize or large deployment, which means that the size is a typical or most common successful deployment for that vendor. Every vendor will have outliers.

SIEM Services

Real-time monitoring and alerting, as well as log collection, query and reporting, are available as a service offering from MSSPs. Gartner customers and MSSPs indicate growing interest in using MSSP to monitor a customer-deployed SIEM. These services are new, and MSSPs will evolve service offerings in two ways. We expect lower-cost template offerings, where the MSSP will configure and tune the SIEM based on a limited number of use cases, with MSSP analysts providing monitoring for selected events, and predefined reporting. We also expect custom offerings, where the MSSP will take over (or share with the customer) monitoring and management of SIEMs, where the customer has established extensive alerting and reporting. We do not include an evaluation of the service delivery capabilities of MSSPs in this Magic Quadrant. However, we do note SIEM product vendors that offer remote management of their SIEM products. Service providers such as Alert Logic and Sumo Logic offer SIEM infrastructure as a service for organizations that do not want to deploy their own SIEM technology.

Return to Top

About Gartner | Careers | Newsroom | Policies | Site Index | IT Glossary | Contact Gartner