G00246886

Magic Quadrant for Security Information and Event Management

Published: 7 May 2013

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

Broad adoption of SIEM technology is being driven by the need to detect threats and breaches, as well as by compliance needs. Early breach discovery requires effective user activity, data access and application activity monitoring. Vendors are improving threat intelligence and security analytics.

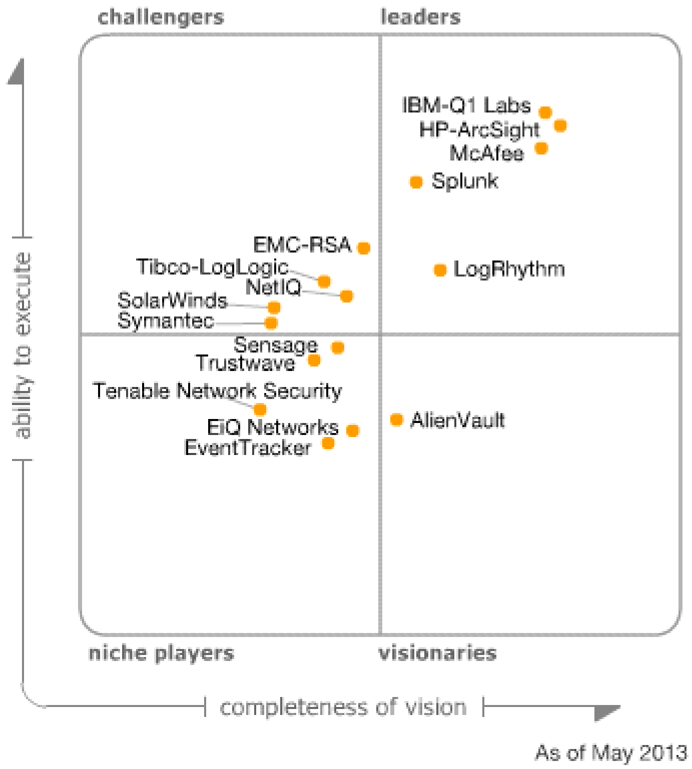
Market Definition/Description

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 incident response, forensics and regulatory compliance. The vendors included in our Magic Quadrant 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 event data produced by security devices, network infrastructures, 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, assets, threats and vulnerabilities. The data is normalized, so that events, data and contextual information from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time security monitoring, historical analysis and other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (May 2013)

Vendor Strengths and Cautions

AlienVault

The foundation for AlienVault's security management solution is Open Source SIEM (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, log management, consolidated administration and reporting, and multitenanting for managed security service providers (MSSPs). AlienVault packages its offering, the AlienVault Unified Security Management platform, into three tiers to match the size of the end user's environment. In every offering provided by AlienVault, all features are enabled. The vendor's target markets are smaller enterprise-class organizations or divisions of larger enterprise organizations that are implementing a security management program and require multiple security technologies at a lower cost and with greater simplicity. During 2012, AlienVault introduced Open Threat Exchange, which enables sharing of Internet Protocol (IP) and URL reputation information. The vendor also released templates that provide contextual incident response guidance. Ease-of-deployment improvements include AlienVault Center, which provides centralized configuration and management of all AlienVault components. There is also an Auto-deploy Dashboard, which leverages asset discovery capabilities to guide log integration.

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, and both host-based and network-based 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

- Predefined correlation rules for intrusion detection system (IDS) and intrusion prevention system (IPS) sources are focused primarily on the suite's Snort sensor data.
- There is no identity and access management (IAM) integration beyond Active Directory monitoring, and application integration is primarily with open-source applications.
- While AlienVault has reduced the need for access to the command line interface for customization and maintenance of the SIEM system itself, some configuration tasks (for example, Snort, OSSEC HIDS and integration of some nonsupported event sources) require the use of the command line interface.

EiQ Networks

EiQ Networks targets enterprise security and compliance buyers with its SecureVue product and also licenses security event management (SEM) technology to MSSPs and 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 augment SIEM with security configuration policy compliance, file integrity monitoring, operational performance monitoring functions and some network behavior analysis capabilities. The vendor has success in the U.S. federal segment and in midsize environments, positioning its suite as a situational awareness platform capable of security monitoring and security configuration assessment.

During 4Q12, EiQ Networks released SecureVue NGS, which is targeted to midsize organizations and provides simplified installation with no customization required. The vendor also expanded integration with threat intelligence feeds and improved data integration capabilities. SecureVue should be considered by organizations that need a combination of SIEM and security configuration assessment in one tool.

Strengths

- SecureVue augments SIEM functionality with additional operational performance, as well as asset and configuration policy compliance capabilities. The vendor 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

- EiQ Networks is a relatively small vendor with low visibility in competitive evaluations.
- Smaller customers indicate that the interfaces for correlation rule building and report customization need to be simplified.

EMC-RSA

RSA, The Security Division of EMC (with enVision, NetWitness and Security Analytics) has one of the largest SIEM installed bases. However, during 2012, competitors continued to identify RSA enVision as the most frequently displaced SIEM technology. Customers report ad hoc query and report performance issues with the enVision platform as primary reasons for considering replacement. RSA has almost completed the transition from enVision to RSA Security Analytics, which incorporates traditional SIEM functionality and is based on the NetWitness platform. RSA Security Analytics provides log and full packet data capture, threat detection, basic security monitoring and basic security analytics. RSA will support the enVision platform until mid-2016. The Security Analytics reporting system can pull data from both the Security Analytics data structures and the Internet Protocol Database (IPDB) in enVision, helping to accommodate the transition from enVision to Security Analytics within the RSA installed base. At the end of 2012, RSA provided an initial release of Security Analytics, including the Security Analytics Warehouse, which supports long-term storage and access for compressed log and network security metadata. The initial release has limitations on analytics (keyword search into raw data), but a release that is planned for 2013 will provide an analytics engine as an integral component of the Security Analytics Warehouse.

NetWitness supports basic threshold monitoring, and this capability is also present in the initial release of Security Analytics. RSA plans a 1H13 general availability release of cross-data-source correlation capabilities for RSA Security Analytics. During 1Q13, RSA released an all-in-one appliance for Security Analytics that is a packaging option for the midmarket.

RSA Security Analytics should be considered by organizations that have deployed enVision and need to overcome query and reporting performance limitations, and also by organizations that need a combination of both log-based monitoring and network-level monitoring for threat detection and investigation.

Strengths

- RSA's Security Analytics platform offers a combination of analytics and basic event monitoring for both full packet capture and log data.
- RSA Security Analytics can be used by current enVision customers as a means of overcoming the query and reporting performance limitations of the enVision platform.
- RSA Security Analytics can be deployed by organizations that have implemented another vendor's SIEM in cases where full packet capture capabilities are needed.

Cautions

- Security Analytics' support for complex correlation was not released at the time of this evaluation.
- RSA support via the Security Analytics Data Warehouse platform for full-function analytics was just introduced at the time this research was written, and there is very little production experience with it.
- The majority of Security Analytics deployments to date have been in large environments with larger-sized security staff, and there is little deployment experience with packaging designed for midsize environments.

EventTracker

EventTracker (formerly Prism Microsystems) targets its SIEM software offering primarily at midsize commercial enterprises and government organizations with security and operations event management and compliance reporting requirements. 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. During 2012, the vendor introduced SIEM Simplified, a set of services (daily incident review, daily or weekly log review, weekly configuration assessment review, incident investigation, and audit assistance), delivered via remote access to the EventTracker instance running on customer premises. Development work continues on plans expressed early in 2012, including a log book function that will provide basic incident tracking, but the new function is not yet released. A redesign of the user interface is also in process. 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 supports centralized agent deployment and management in Windows environments.

- EventTracker includes a behavior analysis module that provides profiling and anomaly detection functions.
- Services such as periodic log review, audit assistance and health check are available from the vendor at a low cost.

Cautions

- The vendor targets the midmarket, but is not as visible on customer shortlists as other SIEM vendors that are also targeting this segment.
- EventTracker's capabilities for application monitoring and integration with IAM products are more limited than other SIEM products targeting enterprise deployments.
- Threat intelligence data is provided as lookup tables and is not integrated with real-time monitoring.
- The imbedded incident ticketing capability is limited when compared with SIEM competitors that lead in this area.

HP-ArcSight

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

During 2011 and 2012, we saw the introduction of competitive SIEM technologies within some large ArcSight accounts, with customers citing ESM complexity and cost as inhibitors to its expansion. During 2011, ArcSight partially addressed these issues for its midsize customers with ArcSight Express version 3, which replaces Oracle Database with the Correlation Optimized Retention and Retrieval Engine (CORR-Engine) and implements a simplified events per second (EPS)-based pricing model. ArcSight extended the CORR-Engine to ESM late in 2012, with the release of ArcSight ESM 6.0c. We have validated a full-scale deployment of this release with an early adopter customer that reported a great improvement in event handling capacity on the same hardware. In 1Q13, HP released Reputation Security Monitor (RepSM) — an optional feed of IP and URL reputation data — from HP Security Research Labs, with 6-hour updates into ArcSight. HP also announced a two-way connector into Autonomy, which provides the ability to flow ArcSight event data into the Autonomy environment to access sentiment and intent analysis from ArcSight. A general two-way Hadoop connector is also available. ArcSight Express should be considered for midsize SIEM deployments. ESM is appropriate for larger deployments, as long as sufficient in-house support resources are available.

Strengths

- ESM 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 SIEM product in competitive evaluations.

Cautions

- ArcSight provides real-time statistical correlation, but profiling and anomaly detection operate against historical data only.
- While the CORR-Engine has eliminated a major source of deployment and support complexity, customers will still find ESM to be more complex than other leading solutions.

IBM-Q1 Labs

IBM's 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 the release of weekly threat intelligence feeds from X-Force. The vendor also introduced QRadar Network Anomaly Detection — designed to complement SiteProtector deployments — adding NetFlow and anomaly detection to the SiteProtector IDS.

IBM has introduced a co-managed service option for QRadar for customers that want to combine an SIEM technology deployment with monitoring services from IBM. This implements an on-premises QRadar deployment that forwards alerts to IBM's MSSP security operations center (SOC) and integrates with the SOC workflow. In 1Q13, IBM announced the integration of QRadar with InfoSphere BigInsights (IBM's commercialized Hadoop offering) and also with IBM's analytics and data visualization technologies. QRadar is a good fit for midsize and large enterprises that need general SIEM capabilities, and also for use cases that require behavior analysis and NetFlow analysis.

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 NetFlow and log events.

Cautions

- Role-based access capabilities for workflow assignment could be improved by providing support for more-granular role definitions.
- QRadar's multitenant support requires a master console in combination with distributed QRadar instances. The number of third-party service providers that offer QRadar-based monitoring services is limited when compared with vendors that lead in this area.

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 6.1 release includes improvements in content update automation that support faster distribution of threat intelligence data to customers. Behavioral profiling was also introduced with this release, as was integration with third-party network forensics technology. Development plans include improvements in network forensics, host forensics and identity intelligence capabilities. LogRhythm is a good fit for midsize and large 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 monitoring 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 vendor's quarterly health check program gets high marks from customers that value the continuing engagement to encourage momentum with security monitoring.
- LogRhythm continues to be very visible in competitive SIEM technology evaluations of Gartner clients.

Cautions

- Although customers report fast response times from LogMart for security-oriented inquiries, indexes are not optimized for IT operations access.
- Active Directory integration for role-based access is present, but only implemented at the individual ID level. Support for Active Directory groups is not yet implemented for role-based access.

McAfee

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 database activity monitoring (DAM) technology.

During 2Q12, McAfee released Enterprise Security Manager 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. The release also includes an integration with Securonix for username normalization. McAfee has also introduced McAfee Event Reporter, which packages Enterprise Security Manager components as a reporting back end for McAfee network, endpoint and security management products. Recent updates include support for automated mitigation and an integration with McAfee Network Threat Behavior Analysis (NTBA) to provide profiling and anomaly detection capabilities for NetFlow data within SIEM. There are plans to build connectors to big data infrastructures, such as Hadoop and Teradata. McAfee Enterprise Security Manager is a good choice for organizations that require high-performance analytics under high-event-rate conditions.

Strengths

- Some of the highest event ingest rates and query performance levels that we have been able to validate have been with McAfee Enterprise Security Manager customers.
- The McAfee Enterprise Security Manager Application Data Monitor (ADM) component provides application and data access monitoring from network-based packet inspection, which augments log-based monitoring.
- The Database Event Monitor (DEM) component of Enterprise Security Manager provides the ability to monitor database activity without a dependence on native audit functions.

Cautions

- Potential users of the ADM component should evaluate their network architecture to determine the required number and availability of monitoring points.
- The flash-driven user interface causes some limitations in expected navigation.

- The risk-based correlation capabilities in the 9.1 release, which was current at the time of this evaluation, are more basic than what is provided by competitors that have implemented profiling and anomaly detection functions. McAfee recently added statistical correlation in the 9.2 release (in April 2013), but the capabilities have not been validated with customer references.

NetIQ

During 2012, NetIQ focused on the consolidation of NetIQ Sentinel (acquired from Novell) with its existing SIEM technology, NetIQ Security Manager. NetIQ's SIEM offering is based primarily on the Sentinel platform, in combination with agent technology and content from Security Manager. NetIQ Sentinel version 7 is composed of three components: the core Sentinel Server; Sentinel Log Manager and Sentinel Agents. Sentinel and Sentinel Log Manager are offered both as software and virtual appliance deployments. NetIQ Sentinel integrates with other core NetIQ technologies (AppManager, Identity Manager, Access Manager, Directory and Resource Administrator, and Secure Configuration Manager). Development plans include broader support for contextual sources and additional application monitoring. Sentinel is a good fit for organizations that require large-scale security event processing in highly distributed environments (such as retail). and is an especially good choice for organizations that have deployed NetIQ IAM infrastructure and need security monitoring with an identity context.

Strengths

- Sentinel and Sentinel Log Manager are appropriate for large-scale deployments that are focused on SEM and threat monitoring.
- The Change Guardian product line provides policy-based privileged user activity monitoring and change detection for Active Directory, Windows, Unix and Linux, as well as file integrity monitoring for host systems.
- NetIQ agent technology can provide guaranteed delivery mechanisms over and above native platform audit functions or agentless methods for use cases that require user and data access monitoring for servers.

Cautions

- NetIQ Sentinel is not visible in competitive evaluations of security monitoring technology.
- Sentinel lacks integration with threat intelligence feeds.
- NetIQ's granular licensing practices can result in complex pricing evaluations and issues during renewal.

Sensage

In September 2012, Sensage was acquired by KEYW, which has been focused on cybersecurity and intelligence services primarily for U.S. government intelligence and defense customers. The company acquired Sensage for its existing footprint in enterprise/commercial sectors. As a component of its Project G strategy, KEYW has indicated plans to continue the Sensage SIEM offering and also to develop the technology as an integration point for its other solutions. For example, KEYW now integrates its threat intelligence (daily update) with Sensage. Customers can pull the content and it can populate Sensage watch lists. The Sensage solution is optimized for precision analytics and compliance reporting for a large event data store. KEYW continues to pursue large deals for specific use cases within verticals such as U.S. and European federal governments, healthcare, 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. Version 5 was released in 4Q12, and updates included real-time monitoring performance improvements. Development plans expressed early in 2012 included a redesign of the user interface, but it has not yet been released. Sensage is a good fit for large organizations with use cases that require security analytics for a large event store with basic real-time monitoring requirements.

Strengths

- Sensage is optimized for large organizations that require high-volume event collection, analytics and reporting for large amounts of log data over long periods for audit, compliance and internal investigations.
- The technology has explicit support for SAP, Oracle (PeopleSoft and Siebel), Lawson, Cerner and other packaged application providers, and the technology is often deployed for a combination of system and application layer monitoring.
- The acquisition by KEYW made additional resources available that are being applied to the further development of the technology, as well as new support, sales and channel resources.

Cautions

- The solution is overly expensive and complex for midsize environments that only require basic log management and reporting functions.
- Sales, marketing and technology packaging is oriented toward larger environments that require large-scale security analytics. Competing solutions are a better fit for midsize organizations with project staffing constraints.
- Although KEYW is primarily a service provider, co-managed service offerings of its Project G solution are not yet generally available. However, a limited number of third-party service providers offer Sensage-based security event monitoring services today.
- KEYW has been oriented to U.S. government agencies and is not visible in commercial markets.

SolarWinds

SolarWinds entered the SIEM market with the 3Q11 acquisition of TriGeo. The vendor repackaged TriGeo's appliance and now sells SolarWinds Log and Event Manager (LEM) software as a virtual appliance. During 2012, SolarWinds made some improvements to the dashboard environment and continued the integration with its other products. There are integrations with SolarWinds' operations monitoring technologies that enable alert forwarding to SolarWinds' operations monitoring consoles and support use cases such as change detection and root cause analysis. Development plans include an expansion of integrations with SolarWinds' portfolio of network and system monitoring products and improvements in profiling and analytics capabilities. SolarWinds LEM is a good fit for small or midsize companies that require SIEM technology that is easy to deploy and those that have already deployed other SolarWinds' operations monitoring components.

Strengths

- SolarWinds LEM is easy to deploy.
- The technology is also well-suited for organizations that have already invested in the vendor's other technology solutions.
- An agent for Windows systems can be used to exert endpoint control and network quarantine functions in response to events observed by the SIEM offering.

Cautions

- SolarWinds LEM is optimized for small to midsize deployments, while other SIEM solutions are a better fit for large-scale deployments.
- The technology lacks support for threat intelligence feeds.
- Some customers have identified a need for better support for "from scratch" creation of scheduled reports.
- The number of service providers that offer SolarWinds LEM-based security monitoring services is limited.

Splunk

Splunk Enterprise provides log management, search, alerting, real-time correlation and a query language that supports over 100 statistical commands. Splunk is widely deployed by IT operations and application support teams for log management analytics, monitoring and advanced search. A bidirectional connector enables data access to Hadoop. The Splunk App for Enterprise Security provides predefined reports, dashboards, searches, visualization and real-time monitoring to support security monitoring and compliance reporting use cases. During the past year, the vendor has become very visible on SIEM evaluation shortlists. In many cases, Splunk has already been deployed by IT operations groups. However, there has also been an expansion in the number of customers deploying the Splunk App for Enterprise Security for stand-alone SIEM use cases.

The Splunk App for Enterprise Security 2.2, released in 4Q12, provides speed and scalability improvements, an interface to add external threat intelligence feeds, parsing support for new data sources (including Oracle logs), and improved analytics for session monitoring (Secure Sockets Layer [SSL] VPN or NetFlow). There are also major reductions in dashboard initialization and refresh times. Development plans include new dashboards to help users see statistical outliers and anomalies for advanced threat detection, improved workflow, and expanded use of threat intelligence feeds to drive threat discovery. Splunk is a good fit for security organizations that require customizable security monitoring and analytics, and is an especially good fit for use cases that span security and operations, and for deployments with a focus on application monitoring.

Strengths

- Splunk's increasing presence in IT operations groups can provide the security organization with early hands-on exposure to its general log management and analytics capabilities, "pre-SIEM" deployment by operations for critical resources, and in-house operations support for an expanded security-focused deployment.
- Splunk's dashboarding and analytics capabilities provide a flexible framework for customization to meet a variety of event management and log management requirements.
- Splunk has built-in support for a large number of external threat intelligence feeds from commercial and open sources.

Cautions

- Data collection with Splunk is easier than many competitors, but monitoring functions require a degree of configuration that makes the solution more appropriate for security organizations with greater-than-average expertise.
- Splunk provides predefined parsing to a more limited set of IAM vendors than some competitors' products. Potential buyers should anticipate customization work to handle the parsing of IAM logs outside Active Directory, LDAP and selected other IAM technologies.
- Reporting capabilities, while improved in the current release, are still more basic than those of many competitors.

Symantec

Symantec typically sells its SIEM technology to its current endpoint protection customers. Symantec Security Information Manager (SSIM) is delivered as a software appliance and provides SIM, SEM and log management capabilities. Symantec has integrated SSIM with Symantec Endpoint Protection (SEP), IT governance, risk and compliance management (IT GRCM) and data loss prevention (DLP) technologies. Symantec also has managed service offerings that use a soft appliance for on-site data collection and analysis. 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's modest enhancements have included support for deployment in a VMware environment, minor improvements to analytics for user activity and improvements in archive/restore policy control. Development plans include the introduction of a unified collection architecture for all Symantec products. SSIM should be considered, along with competing solutions, by organizations that want to integrate DeepSight threat intelligence feeds and that want an SIEM solution that is co-managed by Symantec.

Strengths

- SSIM provides good support for use cases that require a mix of log management, compliance reporting and very scalable security event management functions.
- The SSIM appliance provides SIM, SEM and log management functions that are scalable and easy to deploy. Customers have the option to outsource security monitoring or the management of appliances to Symantec's managed security organization.
- The dynamic integration of Symantec's DeepSight content enables real-time identification of active external threats and known malicious sources.

Cautions

- Symantec has not been very visible in the competitive evaluations of SIEM technology of Gartner clients.
- 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 that are currently supported.
- Symantec has not focused much development attention on the technology during the past few years, and current development plans are modest.
- Deployment assistance from Symantec and other service providers is limited.

Tenable Network Security

Tenable Network Security positions SIEM as a component of its Unified Security Monitoring suite, consisting of the SecurityCenter console, the Log Correlation Engine (LCE) for SIEM, and the Nessus Vulnerability Scanner and Passive Vulnerability Scanner (PVS) products. LCE provides log and event collection, NetFlow monitoring, normalization, analysis, and reporting. SecurityCenter adds the ability to correlate events with data from Nessus and PVS, in addition to threat list intelligence from providers such as IID and ReversingLabs. 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, LCE, Nessus and PVS are available as software, and SecurityCenter, Nessus and PVS are also available as hardware or virtual appliances. Network monitoring is available via the NetFlow and raw traffic monitoring capabilities of LCE, or is enhanced through integration with LCE and the passive network traffic monitoring provided by PVS. The latest version of LCE (4.0) includes full-text indexing and search support, improvements in event rate capacity, and load balancing across LCE instances (which shifts workload to new or underutilized servers). The combination of SecurityCenter and LCE for SIEM and scanning and monitoring via PVS and Nessus provides unified management, monitoring and reporting for SIM, SEM and vulnerability assessment. LCE is a good choice for organizations that want to extend the scope of a Nessus/SecurityCenter deployment to include security monitoring.

Strengths

- The vendor continues to receive strong positive feedback for its technical support.
- The integration of SecurityCenter, LCE, Nessus and PVS provides a single-vendor solution for customers addressing security and compliance requirements that span event and log analysis, vulnerability assessment, and security configuration auditing.
- SecurityCenter and LCE provide statistical analytics, including notification of first-time events and deviations from baseline activity levels.
- Subsequent to the September 2012 funding round, Tenable increased resources for sales, product management, product development, technical support and training.

Cautions

- LCE does not provide support for co-managed SIEM offerings. Prospective customers seeking log integration to support a hybrid SIEM and managed security deployment will need to develop alternative log acquisition methods.
- LCE does not provide integration with IAM policy sources, but is able to extract user identity information from logs.
- LCE does not integrate with major packaged applications.
- SecurityCenter lacks workflow integration with enterprise directories. It provides an internal ticketing capability and can initiate tickets by email to corporate ticketing systems.

Tibco-LogLogic

In April 2012, Tibco Software acquired LogLogic. Tibco has expressed the intention of leveraging its event processing technology to provide scalable security event management functions and also applying its data management and analytics technologies to security use cases. 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 packaged as a software offering. Following the acquisition, integration with Tibco's Spotfire data analytics platform and visualization software was completed. Tibco is pursuing a general development strategy that will provide its large customers with high-end analytics, and complex-event processing through integration of LogLogic with the Tibco portfolio. Long-term plans include the leveraging and repackaging of Tibco components into more tightly integrated, lighter-weight LogLogic components to provide analytics and complex-event processing for security practitioners and IT operations in enterprises and the midmarket. LogLogic is a good fit for use cases focused primarily on log management, or those 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.
- LogLogic 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 database management systems (DBMSs) through the use of specialized agent technology.
- Integration with Spotfire provides high-scale advanced analytics.

Cautions

- LogLogic Security Event Manager does not scale for large deployments.
- 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.
- LogLogic was not very visible in competitive evaluations and we have seen more displacements by SIEM vendors during 2012.

Trustwave

Trustwave's primary business is services for compliance, vulnerability assessment, managed security and security consulting. Its threat and research capability includes SpiderLabs, which provides research on security threats and vulnerabilities in support of service delivery and product development. Trustwave also offers a broad portfolio of security products, including a secure Web gateway, DLP, a Web application firewall, network access control, unified threat management (UTM) and encryption technologies. The core of this portfolio is an SIEM deliverable in several configurations to meet diverse requirements, from large enterprise, SEM-oriented deployments to midsize deployments with more modest SEM needs. The Trustwave SIEM line of log management appliances is Trustwave SIEM, available in three configurations: Log Management Enterprise, Log Management and Log Collector: Software solutions are Trustwave SIEM Enterprise (introduced in January 2013) and Trustwave SIEM Operations Edition (OE). Additional optional components include advanced analytics and agents for event forwarding. The vendor also offers traditional managed security services through its security operations centers running the SIEM OE product, and the Managed SIEM offering that includes customer premises Log Management appliances.

Strengths

- The Trustwave SIEM products include a broad range of deployment formats, capacities and service options for addressing typical SIEM use cases in midsize and large enterprises. These include hybrid product and service options that support customers with limited internal resources for technology management or analysis.

- SIEM OE offers analytics, capacity and customization capabilities appropriate for customers with large-scale event monitoring requirements and the requisite resources to support deployment and ongoing operations.
- Trustwave SIEM and Log Management appliances are suitable for midsize SIEM deployments and distributed environments where ease of deployment and predefined configuration are important requirements.

Cautions

- The variety of options available from Trustwave to mix and match SIEM with their other security products and for managed services means that potential SIEM buyers must carefully scope their requirements to enable like-to-like competitive evaluations against multiple deployment formats for technology, and monitoring and device management services.
- SIEM buyers with requirements to incorporate security technologies from Trustwave's competitors (for example, IPS, DLP and Web application firewall technologies) must monitor the vendor's ability to maintain timely support for these technologies with the Trustwave SIEM products (and services).
- Trustwave is not very visible in competitive evaluations of SIEM among Gartner clients.

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.

Added

- KEYW acquired Sensage.
- Tibco Software acquired LogLogic.

Dropped

The recent acquisitions on the part of HP, IBM, McAfee, EMC-RSA, and NetIQ, and the initial public offering (IPO) of Splunk, have changed the market dynamics. There are now five large vendors that control about 60% of a $1.36 billion market. This has caused Gartner to reconsider both revenue thresholds and the requirements for relative visibility of vendors in the market. The revenue threshold is now $13.5 million per year for 2012 (net new license revenue plus maintenance). Visibility is calculated from the following factors: presence on Gartner client shortlists, presence on vendor-supplied customer reference shortlists, mentions as a competitor by other SIEM vendors and search references on gartner.com.

- CorreLog is an SIEM vendor that no longer meets our more stringent revenue and visibility thresholds.
- Lookwise is an SIEM vendor that was spun out of S21sec, which was included in last year's Magic Quadrant. It has a market presence primarily in Spain and South America. Lookwise does not meet our more stringent revenue and visibility thresholds.
- Tango/04 provides operational event correlation, business process monitoring and SIEM solutions to customers in Europe and South America. The vendor no longer meets our more stringent revenue and visibility thresholds.
- Tier-3 is an SIEM vendor with a presence primarily in the U.K. and Australia; it no longer meets our more stringent revenue and visibility thresholds.

Inclusion and Exclusion Criteria

The following criteria had to be met for vendors to be included in the 2013 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 on the competitive shortlists of end-user organizations.
- They had less than $13.5 million in SIEM product revenue during 2012.
- The solution is delivered exclusively as a managed service.

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 2013)

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. As in last 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, including 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.
  - Analytics are an important capability to support the early detection of targeted attacks and breaches. SIEM vendors have long provided query capabilities against the primary storage tiers of the SIEM technology, and this is the approach that most SIEM customers will use. In order to be effective for early breach detection, the analytics capability must incorporate context about users, assets, threats, and network activity, and must also provide query performance that supports an iterative approach to investigation. Some SIEM vendors are introducing separate "back stores" designed to hold very large amounts of security event, content and contextual data, optimized for analysis. There are also efforts under way to build connectors from the SIEM technology to general purpose "big data" repositories. The "separate analytics back store" approach is being tested by large "type A" companies.

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 include 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.

- **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.
- For **geographic strategy**, although the SIEM market is centered in North America, there is growing demand for SIEM technology in Europe and the Asia/Pacific region, 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 those 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	Standard

Source: Gartner (May 2013)

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 (due to SIEM revenue or SIEM revenue in combination with revenue from other sources). In addition to providing technology that is a good match to current customer requirements, Leaders also show evidence of superior vision and execution for anticipated requirements. They 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.

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. Vendors 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.

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 due to 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.

Niche Players

The Niche Players quadrant is composed primarily of smaller vendors that 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 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.

Context

SIEM technology provides:

- SIM — log management, analytics 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 13 vendors with respect to the three major use cases noted above (see "Critical Capabilities for Security Information and Event Management").

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 (see "Toolkit: Security Information and Event Management RFP").

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 for company-specific deployment scenarios. The requirements definition effort should also 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.

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 increased by 25% over the previous 12 months,[1] and most vendors have reported increases in customers and revenue.[2] During 2012, the SIEM market grew from $1.1 billion to approximately $1.36 billion, achieving a growth rate of about 23%. In North America, there continues to be many new deployments by smaller companies that need to improve monitoring and breach detection. Compliance reporting also continues as a requirement, but most discussions are security-focused. 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. We continue to see large companies that are re-evaluating SIEM vendors to replace SIEM technology associated with partial, marginal or failed deployments. During this period, we have continued to see a stronger focus on security-driven use cases from new and existing customers. Demand for SIEM technology in Europe and the Asia/Pacific region remains strong, driven by a combination of threat management and compliance requirements. As a consequence, our overall evaluation of vendors in this Magic Quadrant includes an evaluation of vendor sales and support strategies for those 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 92% of breaches undetected by the breached organization.[3] 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 expansion of SIEM technology deployments within existing accounts. Several SIEM vendors are beginning to position their technologies as platforms that can provide security, operations and application analytics.

SIEM Vendor Landscape

Sixteen vendors met Gartner's inclusion requirements for the 2013 SIEM Magic Quadrant. Eight are point solution vendors, and eight are vendors that sell additional security or operations products and services. There were two notable acquisitions in the SIEM market since the last SIEM Magic Quadrant: KEYW acquired Sensage, and Tibco Software acquired LogLogic. The SIEM market is now dominated by relatively few large vendors (HP, IBM, McAfee, EMC-RSA and Splunk) that command about 60% of market revenue. Other large vendors such as Symantec and Tibco are also present. A few small vendors continue to do well, but there will be increasing stress on many of the small remaining vendors, The acquisitions on the part of HP, IBM, McAfee, EMC-RSA and NetIQ, and the IPO of Splunk, have changed the market dynamics. We now have five large vendors that control about 60% of a $1.36 billion market. This has caused us to reconsider both revenue thresholds and requirements for relative visibility of vendors in the market. The revenue threshold is now $13.5 million per year for 2012 (net new license revenue plus maintenance). Visibility is calculated from the following factors: presence on Gartner client shortlists, presence on vendor-supplied customer reference shortlists, mentions as a competitor by other SIEM vendors and search references on gartner.com.

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 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 the Asia/Pacific region is becoming increasingly important as SIEM deployments increase in these locations.

Some vendors with broad technology portfolios (HP and IBM) are utilizing SIEM as an integration point for security and operations technologies within their portfolios. Some vendors (IBM, HP, RSA) are also developing integrations with their own big data technologies, while others (McAfee and Splunk) have described integration plans with third-party technologies. A number of vendors with in-house security research capabilities (IBM, HP, McAfee, Symantec and RSA) provide 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 is executing a strategy to provide a common platform (based on NetWitness) for log management and packet capture, and also to integrate with its IT GRCM technology. 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 and competitive visibility levels:

- AccelOps provides security and operations monitoring via a unified log management and event management infrastructure with domain-specific views and analytics. The vendor does not meet our more stringent revenue and visibility thresholds.
- CorreLog is an SIEM vendor that no longer meets our more stringent revenue and visibility thresholds.
- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer.
- Lookwise is an SIEM vendor that was spun out of S21sec and has a market presence primarily in Spain and South America. The distinguishing characteristic of Lookwise is the threat intelligence feeds from S21sec, which are focused on the banking and critical infrastructure sectors. Lookwise does not meet our more stringent revenue and visibility thresholds.
- Tripwire Log Center is focused on augmenting Tripwire capabilities to provide greater system state intelligence.
- Tango/04 provides operational event correlation, business process monitoring and SIEM solutions to customers in Europe and South America. The vendor no longer meets our more stringent revenue and visibility thresholds.
- Tier-3 is an SIEM vendor with a presence primarily in the U.K. and Australia. The distinguishing characteristic of the technology is its profiling and anomaly detection capabilities. The vendor no longer meets our more stringent revenue and visibility thresholds.

A few vendors sell solutions that are based on licensed SIEM technology. IBM licenses its technology to vendors (Juniper Networks and Enterasys Networks) 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 auditing.

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

During the past year, Gartner clients deploying SIEM technology have been primarily focused on security use cases, even though compliance continues to be an important driver. Demand from European clients has remained steady, while the number of Asia/Pacific SIEM inquiries have been rising. Adoption of SIEM technology by a broad set of companies has fostered demand for products that provide predefined security monitoring and compliance reporting 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 Magic Quadrant evaluation, we continue to place greater weight on capabilities that aid in targeted attack detection, including support for user activity monitoring, 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 clients indicate a growing interest in using MSSPs 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 system 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) the monitoring and management of SIEM systems, and 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.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"Critical Capabilities for Security Information and Event Management Technology"

"Planning for an SIEM Technology Deployment"

"How to Deploy SIEM Technology"

"Toolkit: Security Information and Event Management RFP"

"Effective Security Monitoring Requires Context"

Evidence

[1] Based on 350 inquiries during 2012 and 2013 from end-user clients with funded SIEM projects

[2] Based on surveys of 24 SIEM vendors

[3] 2012 Data Breach Investigations Report from Verizon Enterprise Solutions

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets, skills, etc., whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood of the individual business unit to continue investing in the product, to continue offering the product and to advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message in order to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements, etc.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling product that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp