Magic Quadrant for Security Information and Event Management

20 July 2015 ID:G00267505

Analyst(s): Kelly M. Kavanagh, Oliver Rochford

VIEW SUMMARY

The need for early detection of targeted attacks and data breaches is driving the expansion of new and existing SIEM deployments. Advanced users are looking to augment SIEM with advanced profiling and analytics.

Market Definition/Description

This document was revised on 21 July 2015. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The security information and event management (SIEM) market is defined by the customer's need to apply security analytics to event data in real time for the early detection of targeted attacks and data breaches, 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, such as NetFlow and network packet. 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 correlation of events for security monitoring, query and analytics for historical analysis and other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management

EVALUATION CRITERIA DEFINITIONS

Ability to Execute

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

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

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

Market Responsiveness/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 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 initiatives, 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 and so on.

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 to 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 products 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

Source: Gartner (July 2015)

differentiation, functionality, methodology and feature sets 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 vertical markets.

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.

Vendor Strengths and Cautions

AccelOps

AccelOps provides fully integrated SIM and security event management (SEM), file integrity monitoring (FIM), configuration management database (CMDB), and availability and performance monitoring (APM) capabilities. The vendor's primary focus is its SIEM solution for security operations and managed security service providers (MSSPs), but AccelOps also provides a tightly integrated APM solution.

MSSP customers typically use both the SIEM and APM capabilities to provide a broad security and device health monitoring service to their customers. For end-user customers, the focus in most cases is SIEM, but about 25% of end-user customers have added the APM component.

Updates in the last year have included new integrations with open-source and commercial threat intelligence feeds, a new capability to associate remediation activities with specific correlation rules, and the addition of over 200 new report templates. AccelOps has also released Visual Analytics, adding dynamically generated and interactive HTML5 dashboards. An API for workflow integration and bidirectional native support for ServiceNow, ConnectWise, Landesk and Remedyforce have also been added.

AccelOps is a good fit for enterprises and MSSPs that require a combination of security monitoring and APM with integrated CMDB capabilities. It is also well-suited for IT operations teams with a combined operations and security function.

Strengths

- AccelOps' combination of SIEM, FIM and APM capabilities can be used to unify security and operations monitoring from log-based and NetFlow event sources,
- AccelOps has a strong focus on integrating operational and security capabilities to support remediation and incident management.
- The vendor provides strong support for deployment in a virtualized environment, as well as in public, private and hybrid clouds.
- Customers report that the technology is relatively easy to deploy, with positive feedback for the depth and flexibility of customization. The average of AccelOps reference customer satisfaction scores for scalability and performance, predefined reports, report creation and customization, ease and effectiveness of ad hoc queries, product stability, and support experience is higher than the average scores for all reference customers in those areas.

Cautions

- Out-of-the-box support for some third-party security technologies, such as data loss prevention (DLP), application security testing, network forensics and deep packet inspection (DPI), is basic.

The average of AccelOps reference customer satisfaction scores for predefined correlation rules and ease of customizing them is lower than the average scores for all reference customers in those areas.

AccelOps has relatively low visibility in competitive evaluations of SIEM.

AlienVault

The AlienVault Unified Security Management (USM) solution provides SIEM, vulnerability assessment (VA), asset discovery, network and host intrusion detection (NIDS/HIDS), and file integrity monitoring (FIM). AlienVault USM provides centralized configuration and management of all AlienVault components. The AlienVault USM is composed of open-source components, such as OpenVAS (VA), Snort, Suricata (IDS) and OSSEC (HIDS/FIM), and combines these with SIEM to provide a unified security solution. AlienVault also offers open-source SIM (OSSIM), a free, open-source version of its solution with a reduced feature set. AlienVault USM extends OSSIM with scaling enhancements, log management, consolidated administration and reporting, and federation for MSSPs. The vendor also provides the AlienVault Open Threat Exchange and Threat Intelligence. AlienVault's Open Threat Exchange community enables sharing of Internet Protocol (IP) and URL reputation information. AlienVault Labs provides an integrated threat intelligence feed to its commercial products that includes updates to signature, vulnerability, correlation, reporting and incident response content.

AlienVault USM is available as an appliance, software and virtual image, as well as via Amazon Elastic Compute Cloud (EC2). The sensor, logger and server components of USM can be deployed combined in one system (all-in-one architecture), or as separate servers in horizontal and vertical tiers to scale to diverse customer environments.

At the end of 2014, AlienVault released USM for Amazon Web Services (AWS), a purpose-built native EC2 offering providing asset discovery, AWS infrastructure and vulnerability assessment, and Amazon CloudTrail monitoring capabilities, among others. The vendor's target market is enterprises with smaller security staffs and limited security programs that need multiple integrated security technologies at a lower cost and with greater simplicity. The AlienVault USM platform should be considered by organizations that need a broad set of integrated security capabilities at relatively low cost, and by organizations that will accept a commercially supported product that is based on open source.

Strengths

AlienVault USM provides a variety of integrated security capabilities, including SIEM, file integrity monitoring, vulnerability assessment, asset discovery, and both host-based and network-based intrusion detection systems.

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

AlienVault offers a simplified licensing model based on utilized appliances, rather than on events per second (EPS).

The average of AlienVault reference customer satisfaction scores for predefined correlation rules and reports, and the ability to create custom correlation rules, is higher than the average scores for all reference customers in those areas.

Cautions

Although the integrated combined capabilities provide a greater-than-the-parts security posture, they are, in many cases, open source and not best of breed.

Identity and access management (IAM) integration is limited to Active Directory and LDAP monitoring, and application integration is primarily with open-source applications.

AlienVault's workflow capabilities do not include integrations with external directories for workflow assignments.

The average of AlienVault reference customer satisfaction scores for ease of report creation and customization, ease and effectiveness of ad hoc queries, product quality and stability, and support experience is lower than the average scores for all reference customers in those areas.

BlackStratus

BlackStratus has three offerings: Log Storm, SIEM Storm and Compliance Storm. Log Storm provides log management capabilities aimed at MSSPs and small to midsize enterprises, and is available as virtual and hardware appliances. SIEM Storm provides features such as multitenancy and security event management (SEM) capabilities, including analytics, historical correlation and threat intelligence integration, and is deployable as software or virtual images. SIEM Storm can be deployed in combination with Log Storm, utilizing it as the storage and collection tier. Compliance Storm, introduced in 2014, is a cloud-based service for log retention and scheduled reporting for meeting regulatory and compliance mandates.

Log Storm and SIEM Storm provide an integrated incident management and ticketing system guided by the SANS seven-step incident remediation process, and SIEM Storm also allows the tracking of SLA metrics to accommodate MSSP and service-centric environments.

In the past 12 months, BlackStratus has added consolidated cross-tenancy reporting and monitoring. BlackStratus is a good fit for service providers requiring a customizable SIEM platform, and for service-centric end-user organizations looking tor well-formed multitenancy support.

Strengths

Log Storm and SIEM Storm provide a bidirectional integration API to enable custom-built service architectures.

SIEM Storm provides a large selection of out-of-the-box, special-purpose dashboards for roles such as security operations center (SOC) support. Log Storm and SIEM Storm include a fully integrated incident and ticket management system based on the SANS seven-step remediation process.

BlackStratus offers a simplified licensing model based on back-end storage, rather than an EPS-based model.

The average of BlackStratus reference customers satisfaction scores for product quality and stability and support experience are higher than the average scores for all reference customers in those areas.

Cautions

Out-of-the-box support for third-party data sources is limited and may frequently require custom scripting.

BlackStratus has only selective technology integration partnerships or deep third-party integrations.

Advanced security capabilities, such as commercial threat intelligence feeds, network forensic/DPI and IAM integrations, are currently not supported. BlackStratus has focused on sales to security service providers, and has not been very visible in competitive evaluations for end-user deployments.

The average of BlackStratus reference customers satisfaction scores for overall scalability and performance, effectiveness, customization of predefined correlations and reports, and ease and effectiveness of ad hoc queries is lower than the average scores for all reference customers in those areas.

EMC (RSA)

The Security Analytics platform from RSA, The Security Division of EMC, provides visibility from log, full network packet, NetFlow and endpoint data capture. The system performs real-time monitoring and alerting, forensic investigation, analytics, and incident management. The platform includes physical or virtual appliances for data acquisition (Decoders capture and enrich network and log data, Concentrators index data, Brokers aggregate data from Concentrators, and the Event Stream Analysis server does complex correlation, event processing, alerting and incident management). Long-term data storage is provided by Archivers, and the RSA data science models provide complex analysis of historical data. Elements of the solution can be combined in one appliance or distributed to meet customer deployment requirements. A cloud-based feed called RSA Live provides automatic content updates, including correlation rules, reports and threat intelligence feeds.

Recent feature improvements include built-in incident management with workflow capability, support for NetFlow and support for the CEF log format. Other improvements include operational features for easier software upgrades, fault management and health monitoring for the Security Analytics platform.

RSA Security Analytics should be considered by security-conscious organizations that need log-based and network-level monitoring for threat detection and investigation, and have an incident response team (or SOC) or a related service provider for configuring and tuning a complex technology.

Strengths

RSA's Security Analytics platform combines analytics and event monitoring, investigation, and threat intelligence across network packets, NetFlow, endpoints and log data.

Modular deployment options enable customers to select network or event and log monitoring and analysis capabilities as needed.

Integrations with RSA Archer technologies provide additional contextual data, workflow, incident management, run books, reporting, management analytics and metrics to support SOC requirements.

Cautions

The average of RSA reference customer satisfaction scores for scalability, predefined rules and reports, rule and report customization features, ad hoc queries, product quality and stability, and support experience is lower than the average scores for all reference customers in those areas.

The out-of-the-box Security Analytics user interface is basic. The predefined views and dashboards require greater customization than those of competitors.

Security Analytics provides only basic incident management capabilities. Richer workflow capabilities require integrations with RSA Security Operations Management.

EventTracker

EventTracker targets its SIEM software and service offering primarily at midsize commercial enterprises and government organizations with SEM and compliance reporting requirements. EventTracker Security Center is available as software only, and provides SIM and SEM functions. The EventTracker agent provides support for file integrity monitoring and USB control. There are also add-ons available for vulnerability and configuration assessment. 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 any deviations from normal activity. Remediation actions can be executed via a scripting API.

During 2014, EventTracker added support for Threat Intelligence feeds, expanded its Attack Signature feeds and improved support for analyzing application logs. A service offering for on-premises, AWS and Azure installations was also made available for end-user buyers and managed service partners.

Midsize businesses requiring a software-based solution for log and event management, compliance

reporting, and operations monitoring via on-premises or cloud-hosted SIEM, with optional basic monitoring services, should consider EventTracker.

Strengths

- EventTracker is easy to deploy and maintain, with compliance and use-case-specific knowledge packs that provide prebuilt alerts and correlation rules and reports.
- The average of EventTracker reference customer satisfaction scores for scalability and performance, predefined correlation rules and reports, creating and modifying report templates, ad hoc queries, product quality and stability, and technical support is higher than the average scores for all reference customers in those areas.
- EventTracker includes a behavior analysis module that provides profiling and anomaly detection functions.
- Services such as periodic log reviews, audit assistance and health checks 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 lacks integrations with many advanced technologies, such as user behavior analysis, advanced threat detection and network forensics.
- EventTracker's capabilities for application monitoring are more limited than other SIEM products targeting enterprise deployments, as they lack integration with major packaged applications.
- Full incident management, including ticketing, requires an external solution.

HP

HP's ArcSight SIEM solution includes Enterprise Security Manager (ESM) software for large-scale, SEM-focused deployments, and ArcSight Express, an appliance-based offering for ESM 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. HP provides additional modules, such as Application View, providing runtime application visibility based on HP Fortify technology, and HP ArcSight User Behavior Analytics, providing integrated user behavior analysis (UBA) capabilities based on a technology partnership with Securonix. ArcSight licensing is primarily based on consumption in GB per day.

HP added a number of improvements in 2014, notably fully integrated high-availability capabilities for ArcSight ESM, an updated Web UI for ArcSight Logger and enhancements to the ArcSight Management Center that include enhanced health monitoring and distributed management features.

ArcSight Express should be considered for midsize SIEM deployments. ESM is appropriate for large-scale deployments as long as sufficient in-house support resources are available, and for organizations seeking to build a dedicated SOC.

Strengths

- ArcSight ESM provides a complete set of SIEM capabilities that can be used to support an SOC, including a full incident investigation and management workflow.
- HP ArcSight User Behavior Analytics provides true and full UBA capabilities in conjunction with SIEM.
- HP ArcSight has a wide variety of out-of-the-box third-party technology connectors and integrations.
- ArcSight continues to be very visible in competitive evaluations of SIEM technologies.

Cautions

- User feedback indicates that the fat client console UI for ArcSight ESM is considered dated. HP plans to release a Web-based interface in the near future.
- HP ArcSight deployment proposals routinely include more professional services than comparable offerings.
- Customers still provide feedback stating that they find ESM to be more complex than other leading solutions.
- The average of ArcSight reference customer satisfaction scores for scalability and performance, effectiveness of predefined correlation rules and the ease of customizing them, report creation and modification, query capabilities, and product quality and stability is lower than the average scores for all reference customers in those areas. Customer support has been cited as a frequent issue by Gartner clients.

IBM Security

IBM Security's QRadar Platform includes the QRadar SIEM, Log Manager, Vulnerability Manager, Risk Manager, QFlow and VFLow Collectors, and Incident Forensics. QRadar can be deployed as an appliance, a virtual appliance or as SaaS/infrastructure as a service (IaaS). Components can be deployed in an all-in-one solution or scaled by using separate appliances for different functions. The QRadar technologies enable collection and processing of log data, NetFlow data, DPI, full packet capture and behavior analysis for all supported sources.

Recent enhancements include incident forensics support, new data storage appliances, improved query support across logs, flow data, threat intelligence, and vulnerability and asset data. The capability to

replay historical event data through current correlation rules is also now available. IBM plans to improve incident response workflow capabilities, enable sharing of threat intelligence data, and introduce more advanced analytics support for incident investigation and response.

IBM offers a hybrid delivery option for QRadar, with an on-premises QRadar deployment, a SaaS solution hosted on IBM Cloud and optional remote monitoring from IBM's managed security service operations centers. Midsize and large enterprises with general SIEM requirements, and those with use cases that require behavior analysis, network flow and packet analysis, should consider QRadar.

Strengths

- QRadar provides an integrated view of log and event data, with network flow and packets, vulnerability and asset data, and threat intelligence.
- Customer feedback indicates that the technology is relatively straightforward to deploy and maintain in both modest and large environments.
- QRadar provides behavior analysis capabilities for NetFlow and log events.
- The average of IBM reference customers satisfaction scores for scalability and performance, effectiveness of predefined correlation rules, report creation, ad hoc queries, product quality and stability, and technical support is higher than the average scores for all reference customers in those areas.

Cautions

- QRadar provides less-granular role definitions and integrations with enterprise directories for workflow assignment, compared with competitors' products.
- QRadar customers report issues with early versions of QRadar Vulnerability Manager, including limited functionality, instability, late feature updates and support delays.

Intel Security

Intel Security provides McAfee Enterprise Security Manager, which combines SIM and SEM functions, and is available as a physical, virtual or software appliance. The three primary components that make up the SIEM offering are the Enterprise Security Manager, the Event Receiver (ERC) and the Enterprise Log Manager, which can be deployed together as one instance, or separately for distributed or large-scale environments.

Capabilities can be extended and enhanced with a range of specialized add-on products, such as Advanced Correlation Engine (ACE), Database Event Monitor (DEM), Application Data Monitor (ADM), and Global Threat Intelligence (GTI).

Among the enhancements released in the past 12 months were support for AWS deployment and new dashboards for risk analytics and cyberthreat management, as well as improved case and incident management capabilities. McAfee Enterprise Security Manager also released an integration with McAfee's Advanced Threat Defense (ATD) and Threat Intelligence Exchange (TIE) for advanced threat monitoring and defense.

McAfee Enterprise Security Manager is a good choice for organizations that utilize other Intel Security technologies, as well as those seeking an integrated security framework that includes advanced threat defense or monitoring of industrial control systems.

Strengths

- Out-of-the-box third-party device support is cited as a strength by end users. The average of Intel Security reference customers satisfaction scores for scalability, report customization, ad hoc queries and support experience is higher than the average scores for all reference customers in those areas.
- Deep integrations with Intel Security's Enterprise Security Database Event Monitor and Application Data Monitor provide in-depth database and application monitoring for selected technologies.
- Enterprise Security Manager has strong support for monitoring operational technology (industrial control systems [ICSs]), and supervisory control and data acquisition (SCADA) devices.
- Customers report that integrating multiple McAfee security products often yields good synergies and provides better solutions than were otherwise available.

Cautions

- Intel Security's many advanced SIEM features and capabilities in areas such as endpoint intelligence and automated response require integrations with, or further investments in, other Intel portfolio products. Some require ePolicy Orchestrator (ePO) to act as middleware.
- NetFlow can be used to generate events and alerts, but is not automatically used to enrich log-based events.
- User feedback indicates that version 9.4.x has been troubled by some stability and performance issues. The average of Intel Security reference customers satisfaction scores for predefined correlation rule effectiveness and customization, predefined reports and new report creation, and product quality and stability is lower than the average scores for all reference customers in those areas.

LogRhythm

LogRhythm sells its appliance- and software-based SIEM solutions to midsize and large enterprises. LogRhythm's SIEM consists of several unified components: the Event Manager, Log Manager, Advanced Intelligence Engine (AI Engine) and Console. For distributed log collection, Site Log Forwarders are

available, and an agent is also provided for Linux, Unix and Windows for local log collection. Network forensic capabilities such as DPI, NetFlow monitoring and full packet capture are supported via LogRhythm's Network Monitor. LogRhythm's System Monitor Agents include basic host activity monitoring capabilities such as system process monitoring; file integrity monitoring for Windows, Linux and Unix; and Windows registry monitoring.

In the past year, LogRhythm has added a new incident response and case management workflow capability that includes a centralized evidence locker and incident response collaboration tools. It has also expanded the scope of supported devices for log normalization and applications for network monitoring. The AI Engine has been updated to include risk-based profiling and behavioral analytics to identify statistical anomalies for network, user and device activity.

LogRhythm is an especially good fit for organizations that require an integrated combination of SIEM, endpoint and network monitoring capabilities, and those organizations that value ease of deployment and predefined function over a "build your own" approach to monitoring.

Strengths

- LogRhythm combines SIEM capabilities with endpoint monitoring, network forensics and incident management capabilities to support security operations use cases.
- Gartner receives consistent user feedback stating that LogRhythm's solution is straightforward to deploy and maintain, and provides effective out-of-the-box use cases and reporting templates.
- The average of LogRhythm reference customers satisfaction scores for scalability and performance, effectiveness of predefined rules, usefulness of predefined reports, ease of use and effectiveness of predefined queries, product quality and stability, and support experience support is higher than the average scores for all reference customers in those areas.
- LogRhythm continues to be very visible in the competitive SIEM technology evaluations of Gartner clients.

Cautions

- User feedback indicates that creating new reporting templates could be more intuitive.
- Users report that options for reporting focused on alert trending are limited.

Micro Focus (NetIQ)

In November 2014, Micro Focus acquired NetIQ (as part of Attachmate). In April 2015, Micro Focus announced that the NetIQ products would be brought into the Micro Focus portfolio; branding and packaging changes for SIEM and other products may occur in 2015. NetIQ SIEM is composed of three packages: Sentinel, Sentinel Log Manager and Change Guardian. Optional host monitoring agents are also available. Sentinel and Change Guardian are offered both as software and virtual appliance deployments. Sentinel integrates with other core NetIQ technologies (AppManager, Identity Manager, Access Manager, Directory and Resource Administrator, and Secure Configuration Manager). NetIQ made modest enhancements to Sentinel during the past 12 months. Development plans include more support for large-scale data storage and analytics, enhancement and extension of current analytics, better visualization and user interfaces, and support for threat exchange formats.

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.
- Integrations with other NetIQ technologies provide capabilities to support user monitoring, identity and endpoint monitoring, and enforcement/response use cases.
- 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.
- NetIQ customers give Sentinel above-average or average marks for report creation and customization, and ease of ad hoc queries.

Cautions

- NetIQ Sentinel has low visibility in competitive evaluations of SIEM among Gartner clients.
- NetIQ provides generic capabilities to pull data for context, as well as to import from big data repositories. However, it does not provide specific integrations with solutions such as entity behavior analytics platforms.
- NetIQ has a generic ability to integrate threat intelligence feeds, as well as packaged support for open-source feeds (e.g., malware) and Webroot. However, support still lags behind competitors.
- Usability and reporting of the results when replaying historical event data against correlation rules are limited when compared with some competitors.
- The average of NetIQ reference customer satisfaction scores for scalability and performance, correlation rule customization, usefulness of predefined reports, effectiveness of ad hoc queries, product quality and stability, and support experience is lower than the average scores for all references across those areas.

SolarWinds

SolarWinds Log & Event Manager (LEM) software is a virtual appliance. SolarWinds positions LEM as an

easy-to-deploy and use SIEM for resource-constrained security teams that have no requirements for big data advanced analytics or malware detection integration. LEM has integrations with SolarWinds' other products for operations monitoring to support activities such as change detection and root cause analysis. SolarWinds LEM is a good fit for small or midsize companies that require SIEM technology that is easy to deploy, and for those that use other SolarWinds operations monitoring components.

Strengths

- SolarWinds LEM is easy to deploy and provides extensive content in the form of dashboards and predefined correlation rules and reports.
- The technology is well-suited for organizations that have already invested in the vendor's other technology solutions.
- A SIEM autoresponse capability for endpoint USB and quarantine control is available via an agent for Windows systems.
- The average of SolarWinds reference customer satisfaction scores for overall scalability and performance, effectiveness of predefined rules, usefulness of predefined reports, product quality and stability, and support experience is higher than the average scores for all references across those areas.

Cautions

- SolarWinds LEM provides basic statistical and behavior analytics, but has no integration with user behavior analysis tools or with data warehouse technologies. LEM can obtain alerts from a limited number of malware detection or "sandboxing" technologies.
- Customers requiring more extensive user and application or Web monitoring must acquire other SolarWinds products to extend the capabilities available in LEM.
- Although LEM includes a native flow capture and display capability, flow data is not available for real-time correlation in LEM, and packet capture is not supported.

Splunk

Splunk Enterprise and Splunk Cloud provide search, alerting, real-time correlation and a query language that supports visualization using more than 100 statistical commands. Splunk is widely deployed by IT operations and application support teams for log management, analytics, monitoring, and advanced search and correlation. In many cases, the presence of Splunk for operations support leads to consideration of the technology for SIEM, and Gartner customers regularly include Splunk on shortlists for SIEM. 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.

Splunk has continued to enhance the App for Enterprise Security, predefined security indicators and dashboards and visualizations, as well as to improve support for wire data capture and analysis. New advanced query and data pivot enable easier access to functions previously available only through the Splunk query language. Splunk can be deployed for SIEM as on-premises software, in a public or private cloud, as a SaaS offering from Splunk (Splunk Cloud), or in any combination (hybrid).

Splunk supports a broad range of threat intelligence feeds, including STIX/TAXII formats for importing and sharing feeds. Organizations that require an SIEM platform that can be customized to support extensive analytics functions and a variety of log formats, and those with use cases that span security and IT operations support, should consider Splunk.

Strengths

- Splunk's strong presence in IT operations groups can provide security organizations 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 expanded security-focused deployments.
- Splunk customers cite visualization and behavioral, predictive and statistical analytics as effective elements of advanced monitoring use cases, such as detecting anomalous user access to sensitive data.
- Splunk has enhanced built-in support for a large number of external threat intelligence feeds from commercial and open sources.
- The average of Splunk reference customer satisfaction scores for scalability and performance, effective and useful predefined rules and reports, rule and report customization features, report creation, ease and effectiveness of ad hoc queries, product quality and stability, and support experience is higher than the average scores for all reference customers in those areas.

Cautions

- The Splunk App for Enterprise Security provides basic support for predefined correlations for user monitoring. Potential buyers should anticipate modifying those and building their own to implement more advanced user monitoring use cases.
- Workflow and case management functions lag behind those of competitors. Organizations with mature SOC processes may require customization or integrations with third-party technologies for these functions.
- Splunk's license model is based on data volume indexed per day. Customers report that the solution is more costly than other SIEM products where high data volumes are expected.

Trustwave

In April 2015, The Singtel Group (Singtel) announced its intent to acquire Trustwave, and that

Trustwave will continue to operate as a stand-alone business. At the time of this writing, the deal is pending regulatory approval. Trustwave's primary business is managed security services, vulnerability assessment and compliance services. Trustwave also offers a broad portfolio of security products, including secure Web and email gateways, DLP, a Web application firewall, network access control, unified threat management (UTM), security scanning, 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.

Trustwave has three SIEM product options: Log Management Appliances, SIEM Enterprise and SIEM Operations Edition (OE). SIEM Enterprise and Log Management Appliances are available as physical or virtual appliances. In 2014, Trustwave deployed UI and dashboard improvements and upgraded hardware offerings, as well as further integration of its Threat Correlation Service into the Log and SIEM products.

Trustwave is a good fit for midsize organizations seeking SIEM as a full portfolio of technologies and service options for meeting threat management and compliance requirements.

Strengths

- The acquisition by Singtel should result in better access to sales and support functions in the Asia/Pacific region and other markets where Singtel has a presence and brand recognition.
- The Trustwave SIEM products include a broad range of deployment formats and service options, including hybrid options that support customers with limited internal resources for technology management or security analysis.
- SIEM Enterprise offers correlation, capacity and customization capabilities appropriate for customers with large-scale event monitoring requirements.
- Trustwave's self-healing network offering leverages Trustwave's SIEM products to provide autoresponse capabilities such as quarantining and blacklisting.
- The average of Trustwave reference customer satisfaction scores for ease of customizing correlation rules and report templates is higher than the average scores for all reference customers in those areas.

Cautions

- Trustwave is not very visible in competitive evaluations of SIEM offerings among Gartner clients.
- Support for external data warehouse or big data technologies is under development, but not yet available for Trustwave's SIEM offerings. The vendor lags behind competitors in supporting the monitoring of cloud environments. Trustwave's SIEM products do not support Amazon CloudTrail or platform-as-a-service environments.
- The average of Trustwave reference customer satisfaction scores for scalability and performance, effectiveness of predefined rules, usefulness of predefined reports, creating new reports, ease and effectiveness of ad hoc queries, product quality and stability, and overall support experience is lower than the average scores for all reference customers in those areas.
- Customers should monitor Trustwave's SIEM roadmap to ensure that development priorities remain aligned with customer expectations in the wake of the planned acquisition by Singtel.

Vendors Added and 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's appearance 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. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

No vendors were added to the Magic Quadrant.

Dropped

- TIBCO Software is no longer positioning its LogLogic product as an SIEM.
- Tenable Network Security's Security Center and Log Correlation Engine are now positioned as complementary technologies to SIEM. These products can support some SIEM use cases, but are not sold or marketed as SIEMs.

Inclusion and Exclusion Criteria

The following criteria had to be met for vendors to be included in the 2015 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 2014.

The solution is delivered exclusively as a managed service.

SIEM is a $1.69 billion market that grew 12.5% during 2014, with an expected growth rate of 10.9% during 2015. For exclusion, Gartner considers revenue and relative visibility of vendors in the market. The revenue threshold is $13.5 million per year for 2014 (net new license revenue plus maintenance). Visibility is calculated from the following factors: presence on Gartner client shortlists via client inquiries, search references on gartner.com, presence on vendor-supplied customer reference shortlists and mentions as a competitor by other SIEM vendors.

Evaluation Criteria

Ability to Execute

Product or service evaluates the vendor's ability and track record to provide product functions in areas such as real-time security monitoring, security analytics compliance reporting and deployment simplicity.

Overall viability includes an assessment of the technology provider's financial health, the financial and practical success of the overall company, and the likelihood that the technology provider 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/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 and service experience 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 or Service	High
Overall Viability	High
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (July 2015)

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 early targeted attack and breach detection, and simplified implementation and operation, while also meeting compliance reporting 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 an evaluation of 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 the relative ratings of vendors with capabilities in these areas, but there would be a severe vision penalty for a vendor that has

shortcomings in this area. We continue to place greater weight on current capabilities that aid in targeted attack detection, including:

- Vendor capabilities for profiling and anomaly detection to complement existing rule-based correlation.
- Threat intelligence integration, which includes automated update, filtering, and usage within rules, alerts and reports.
- 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. We also evaluate predefined analytics for user behavior analysis.
- Data access monitoring capabilities, which include direct monitoring of database logs and integration with database audit and protection products, DLP integration, and file integrity monitoring through 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, 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 SIEM technology. 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 have introduced separate "back stores" designed to hold very large amounts of security event, content and contextual data, optimized for analysis. A number of SIEM vendors have also built connectors from the SIEM technology to general-purpose big data repositories. Initial deployments of the "separate analytics back store" approach have been implemented by a small number of Type A companies.
- Inclusion of advanced threat detection, network monitoring and packet capture capabilities, and integrations with third-party technologies that provide these functions for more effective early breach detection.

Despite the vendor focus on expansion of capability, we continue to heavily weight deployment simplicity. Users, especially those with limited IT and security resources, still value this attribute over breadth of coverage beyond the core use cases. SIEM products are complex and tend to become more so as vendors extend capabilities. Vendors that are able to provide effective products that users can successfully deploy, configure and manage with limited resources will be the most successful in the market.
We evaluate options for co-managed or hybrid deployments of SIEM technology and supporting services because a growing number of Gartner clients are anticipating or requesting ongoing service support for monitoring or managing 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 queries and analytics, capabilities/plans for profiling and anomaly detection, and threat intelligence. There is also an evaluation of technology capabilities for monitoring cloud workloads.

For **Geographic strategy,** although the North American and European SIEM markets produce the most revenue, Latin America and the Asia/Pacific region are growth markets for SIEM and are driven primarily by threat management and secondarily by compliance requirements. 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	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Not Rated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (July 2015)

Quadrant Descriptions

Leaders

The SIEM Leaders quadrant is composed of vendors that provide products that are a strong 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 emerging and 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 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. As the SIEM market continues to mature, the number of Challengers has dwindled. Vendors in this quadrant would typically have strong execution capabilities, as evidenced by financial resources, a significant sales and brand presence garnered from the company as a whole, or from other factors. However, Challengers have not demonstrated a complete set of SIEM capabilities or they lack the track record for competitive success with their SIEM technologies, compared with vendors in the Leaders quadrant.

Visionaries

The Visionaries quadrant is composed of vendors that provide products that are a strong 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 vendors that provide SIEM technology that is a good match to a specific SIEM use case or a subset of SIEM functional requirements. Niche Players focus on a particular segment of the client base (such as small businesses, service providers, or a specific geographic region or industry vertical) or may provide a more limited set of SIEM capabilities. In addition, 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 more narrowly focused markets or use cases.

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
- An SIEM 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 continues to more heavily weight capabilities that support targeted attack detection. As a companion to this research, we evaluate the SIEM technologies of the vendors in this Magic Quadrant 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 24% over the previous 12 months, and most vendors have reported increases in customers and revenue. During 2014, the SIEM market grew from $1.5 billion to approximately $1.69 billion, achieving a growth rate of about 14%. The primary drivers that were in place at the start of 2014 remain in effect. Threat management is the primary driver, and compliance remains a secondary driver. 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 with Gartner clients are security-focused. There continue to be 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 steady, driven by a combination of threat management and compliance requirements. Growth rates in Asia and Latin America are much higher than those in the U.S. and Europe. 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. The situation can be improved with stronger threat intelligence, the addition of behavior profiling and better analytics. We are monitoring the emerging entity behavior analysis (also called entity behavior analysis, and sometimes called UBA) market, as early adopters report effective detection of targeted attacks with limited deployment efforts. We expect SIEM vendors to increase their support for behavior analysis capabilities and predefined content over the next 18 months. Most companies expand their initial SIEM deployments over a three-year period to include more event sources, greater use of real-time monitoring and investigation to support incident response. The large SIEM vendors have significant existing customer bases, and there continues to be a focus on the expansion of SIEM technology deployments within existing accounts. In general, SIEM vendors are continuing to incrementally improve product capabilities in areas related to breach detection — threat intelligence, anomaly detection and activity monitoring from the network — as well as investigation workflow and case management.

SIEM Vendor Landscape

Fourteen vendors met Gartner's inclusion requirements for the 2015 SIEM Magic Quadrant. Six are point solution vendors, and eight are vendors that sell additional security or operations products and services. There were no notable acquisitions in the SIEM market during 2014. The SIEM market continues to be dominated by relatively few large vendors — HP, IBM, Intel Security and Splunk — that command more than 60% of market revenue. LogRhythm is an example of a point solution vendor that continues to do very well, but there is increasing stress on many of the remaining small vendors.

There has been some additional market consolidation over the past 18 months. Symantec announced the end of sale of its SIEM technology as of 2 September 2014, and the end of support as of November 2017. Tenable Network Security and TIBCO Software join the list of vendors that no longer position their technology competitively in the SIEM market, but are appropriate for select use cases and as providing adjunct capability to SIEM. We maintain revenue thresholds and relative visibility requirements for inclusion of vendors in the market. The revenue threshold is $13.5 million per year for 2014 (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.

SIEM technology is now deployed by a broad set of enterprises. 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, but most SIEM purchases are made on the merits of SIEM capabilities. Many SIEM vendors continue to develop sales channels that can reach the midsize market in North America. Sales effectiveness in Latin America and the Asia/Pacific region is also a focus.

SIEM vendors have responded to the customer focus on targeted attack and breach detection through incremental development of SIEM capabilities in areas such as threat intelligence, analytics, profiling and anomaly detection, and network activity monitoring (both NetFlow analysis and full packet capture). However, we have observed the emergence of user behavior analytics point solution vendors that are providing advanced capabilities in the area of early breach detection, with "signal to noise ratios" that are much better than what has been achieved by SIEM vendors.

Some vendors (IBM, HP and RSA) are also developing or have deployed integrations with their own big data technologies, while others (Intel Security and Splunk) have integrated with third-party technologies. A number of vendors with in-house security research capabilities (IBM, HP, Intel Security, RSA and Trustwave) provide integration with proprietary threat intelligence content. Vendors that have both SIEM and MSSP businesses (HP, IBM, Trustwave and EventTracker) are marketing co-managed SIEM technology deployments that include a range of monitoring services. RSA provides a common platform for log management and network packet capture, and also integrates its SIEM with its IT governance risk and compliance management (GRCM) technology. Intel Security's strategy is increasingly focused on technology integration within its own security portfolio and selling SIEM to large enterprises that use its endpoint security products. Several vendors are not included in the Magic Quadrant because of a specific vertical market focus and/or SIEM revenue and competitive visibility levels:

- FairWarning provides privacy breach detection and prevention solutions for the healthcare market that entail user activity and resource access monitoring at the application layer, and has expanded to include security monitoring for Salesforce.
- 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's 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.
- Huntsman Security (part of 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 does not meet our more stringent revenue and visibility thresholds.

A few vendors sell solutions that are based on licensed SIEM technology. IBM licenses its technology to a few vendors that implement its technology on their own appliances, and add specific integrations with their respective management infrastructures.

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

During the past year, Gartner clients deploying SIEM technology have continued to be primarily focused on security use cases, even though compliance continues to be an important driver. The primary focus continues to be targeted attack and breach detection. 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.

Demand from North American and European clients has increased, while the number of Asia/Pacific SIEM inquiries has remained steady as a percentage of total SIEM inquiry activity. The continued adoption of SIEM technology by companies with limited security programs has fostered a demand for products that provide predefined security monitoring and compliance reporting functions, as well as ease of deployment and support.

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 threats, 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.

Scalability

Scalability is a major consideration in 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.

Gartner defines a small deployment as one with 300 or fewer event sources, a sustained EPS rate of 1,500 events per second or less, and a back store sized at 800GB or less. Gartner defines a midsize deployment as one with 400 to 800 event sources, a sustained event rate of 2,000 to 7,000 events per second and a back store of 4TB to 8TB. A large deployment is defined as one with more than 900 event sources, a sustained event rate of more than 15,000 events per second, and a back store of 10TB or more. Some very large deployments have many 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

Gartner customers increasingly indicate that they are seeking external service support for their SIEM deployment, or are planning to acquire that support in conjunction with an SIEM product. Drivers for external services include lack of internal resources to manage an SIEM deployment, lack of resources to effectively monitor the alerts or do so 24/7, or lack of expertise to expand the deployment to include new use cases (such as user activity monitoring). We expect demand by SIEM users for such services will grow, as more customers adopt 24/7 monitoring and implement use cases that require deeper SIEM operational and analytics expertise.

SIEM vendors may support these needs with managed services, with staff augmentation or outsourcing services, or via partners. Managed security service providers, which offer real-time monitoring and analysis of events, and collect logs for reporting and investigation, are another option for SIEM users. The number of hosted SIEM, or SIEM as a service offerings (such as Splunk Cloud and Alert Logic, and log services from Sumo Logic), is increasing to support customers opting to forgo SIEM technology management, but able to use internal resources for monitoring and investigation. Customer-specific requirements for event collection and storage, alerting, investigation, and reporting may prove problematic for external service providers, and SIEM users exploring services should evaluate the fit of the service provider to meet current and planned use cases.