Magic Quadrant pour les informations de sécurité et la gestion des événements

Publié le 10 octobre 2022 - ID G00 755317 - 49 min de lecture

Par Pete Shoard , Andrew Davies , **et 1 de plus**

Les responsables de la sécurité et de la gestion des risques ont toujours besoin d'un système d'enregistrement de la sécurité doté de capacités complètes de détection des menaces, d'investigation et de réponse. SIEM évolue vers une plate-forme de sécurité avec de multiples fonctionnalités et modèles de déploiement. Cette recherche vous aidera à trouver la bonne solution.

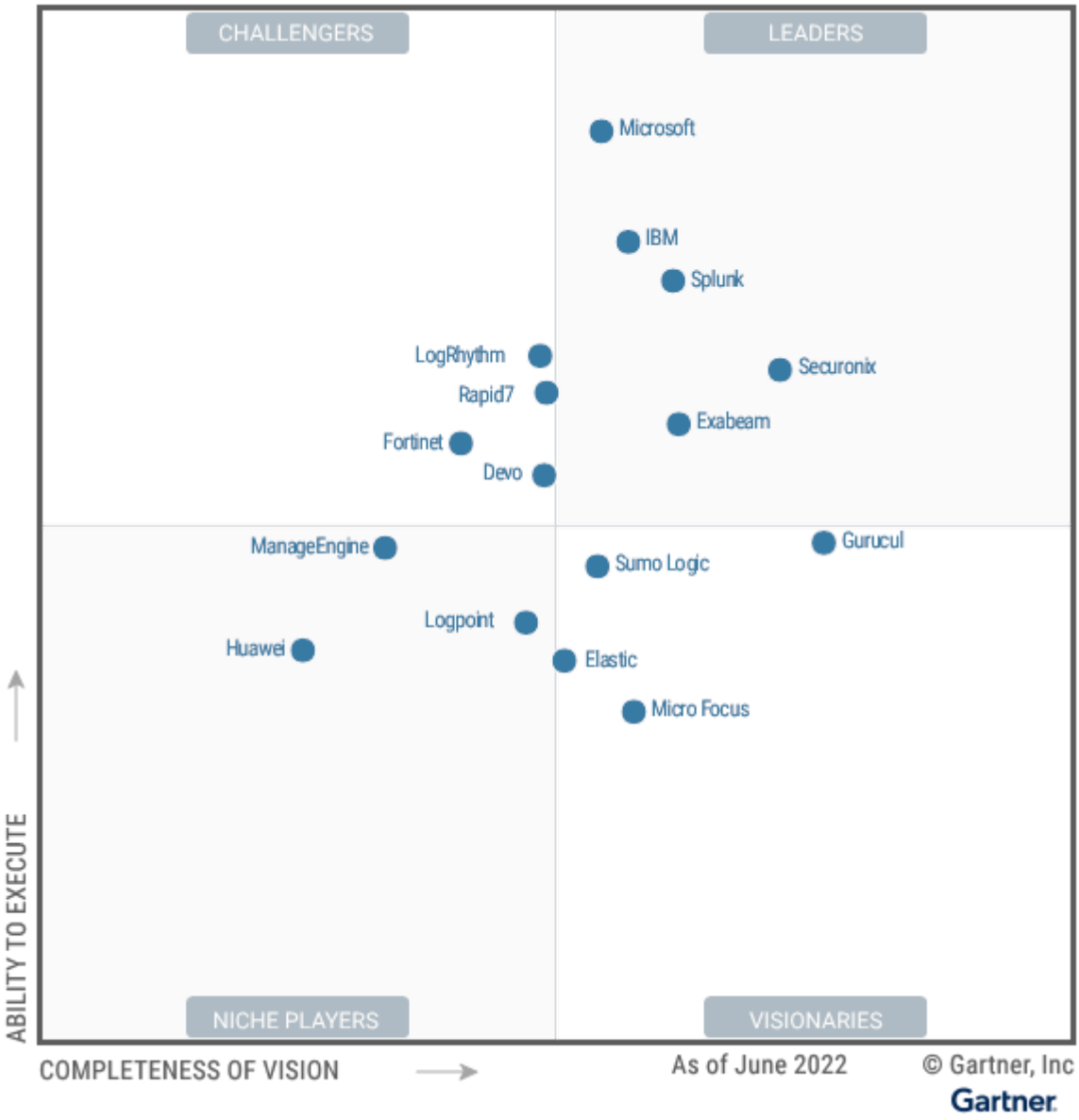
Définition/Description du marché

Ce document a été révisé le 12 octobre 2022. Pour plus d'informations, consultez la page Corrections sur gartner.com.

SIEM agrège les données d'événement produites par les solutions de surveillance, d'évaluation , de détection et de réponse déployées dans les environnements d'application, de réseau, de terminaux et de cloud. Les fonctionnalités incluent la détection des menaces, via la corrélation et l'analyse du comportement des utilisateurs et des entités (UEBA), et les intégrations de réponse généralement gérées via l'orchestration, l'automatisation et la réponse de la sécurité (SOAR). Les rapports de sécurité et le contenu des menaces mis à jour en permanence via la fonctionnalité de la plateforme de renseignements sur les menaces (TIP) sont également des intégrations courantes . Bien que SIEM soit principalement déployé en tant que service basé sur le cloud , il peut prendre en charge le déploiement sur site.

Quadrant magique

Figure 1 : Magic Quadrant pour la gestion des informations de sécurité et des événements



Points forts et mises en garde du fournisseur

Dévo

Devo is a Challenger in this Magic Quadrant. Its SIEM product, the Security Operations application, is delivered as a SaaS offering. Devo's SIEM customer base is primarily in North America, followed by Europe and the Middle East, and is made up of small, midsize and enterprise organizations. Early in 2022, Devo achieved "In Process" status for the Federal Risk and Authorization Management Program (FedRAMP) standard, and expects to reach full authorization later in the year. Licensing, including its add-on capabilities (TIP via MISP, hot storage, Entity Analytics and Devo Flow), is based on the volume of data ingested.

Strengths

- **IT observability coupled with security:** Devo delivers IT observability and security capabilities within the same UI and provides strong timelines, as well as adjacent views for joint functionality across security and I&O teams.
- **Accessibility of data:** Devo's SIEM tool allows users to quickly and easily send data into the solution via its API at any point in which all of that data is indexed. Therefore, customers can access the data whenever, wherever and can leverage the data any way they need to.

- **Native TIP features:** Devo provides TIP functionality via MISP at no additional charge, which uses a multitude of publicly available feeds and sends the intelligence to the SIEM tool for enrichment and enhanced detections.

Cautions

- **Lacks native SOAR functionality:** Devo's SIEM solution integrates with many visible SOAR vendors in the market; however, it does not currently offer the response components of a SOAR.
- **Limited visibility in the SIEM market:** Although Devo has increased its sales operations and expanded its marketing campaigns, it is not as well-known in the SIEM market as some of its competitors.
- **Limited security service support:** External support for Devo's SIEM solution from MSSPs/MDR providers is limited when compared to other SIEM vendors in the market. Customers needing managed or co-managed SIEM services should ensure that their chosen provider can support the Devo SIEM and build additional custom content to improve the rules delivered by Devo.

Elastic

Elastic is a Visionary in this Magic Quadrant. Its Elastic Security solution is mainly focused on security analytics and enterprise search functionality coupled with the Elastic Endpoint security agent, which is included with the SIEM solution. The majority of Elastic Security clients are in North America and Europe, with an equal mix of small, midsize and enterprise clients. New customer growth is currently higher among small organizations. In 2021, Elastic completed its acquisition of Cmd and build security to offer cloud workload protection platform functionality within the Elastic Agent included with Elastic Security. Licensing is based on cloud resources such as compute and storage to support the client environment.

Strengths

- **Custom visualization:** Elastic is known for highly customizable dashboards and creating preferential views of data for analysis purposes. Users can use the combined IT observability and security functionality within the same view for unique timeline and adjacent-activity views.
- **Search functionality:** Elastic Security uses its popular search capability and query language, which is also used as the back-end search and query engine by other SIEM vendors, to aid security operations tasks such as threat hunting. Elastic's ability to parse and index virtually any part of a log gives security operators unlimited options to search and slice any data that has been indexed.
- **Collaboration and notification integrations:** Elastic uses Actions and Connectors to integrate with multiple collaboration tools, ticketing systems and notification tools. Buyers looking for a SIEM that can integrate with their incident collaboration tool of choice will find that Elastic Security supports integration with many popular third-party solutions.

Cautions

- **Native modern SIEM features:** Elastic Security does not offer native SOAR within its SIEM solution, relying instead on partner integrations with other SOAR vendors and offering some response actions with Elastic Agent. No TIP capability exists within the solution, a feature that appears in an increasing number of competing solutions.

- **Support for third-party EDR:** Elastic Security supports data collection from major EDR providers. However, bidirectional support for non-Elastic EDR vendors must be configured using Elastic's generic REST connector.
- **Compliance reporting:** Elastic Security does not offer support for alerting and reporting on compliance standards. Buyers will need to find alternative solutions for compliance reporting.

Exabeam

Exabeam is a Leader in this Magic Quadrant. Exabeam's SaaS SIEM solution, known as Exabeam Fusion SIEM, is available as a core product or bundled with enterprise versions. These products are also available for hybrid cloud. The enterprise version includes Advanced Analytics, Threat Hunter, Entity Analytics and Case Manager. Extra cloud data storage (Cloud Archive) and an Incident Responder (SOAR) are available as add-ons. The majority of Exabeam customers are in North America, with the next-largest concentration in Europe. Most customers are large enterprises, however midsize and smaller client volumes are increasing. Licensing is term-based and depends on the data volumes ingested.

Strengths

- **Long-term, searchable log storage:** The combination of Exabeam Cloud Archive (for up to 10-year data retention), search across normalized events, anomalies, indicators of compromise, and a timeline of log events with automated enrichment enables hunting and investigation supported by rich context over long time frames.
- **Live access to third-party data:** Exabeam Fusion SIEM is able to display and process live data from third-party systems (such as threat intel feeds), enabling the SIEM to operate in a more decentralized fashion for certain use cases. Data decentralization enables more cost-effective deployments, with more up-to-date data, which is expected to be a key trend for SIEM over the next 18 months.
- **Effective alert prioritization:** Dynamic scoring enables clients to surface high-interest discoveries from third-party alerts (in addition to Exabeam's own alerting) using contextualization and analytical models in real time. This allows security analysts to achieve a prioritized view on all alerts generated across their entire security technology stack.

Cautions

- **Lack of native ecosystem components:** Exabeam relies on third-party EDR and NDR. This lack of native capability trails some competitors in the market and reduces its ability to natively respond to threats without further investment in compatible toolsets.
- **Confusing messaging around Fusion XDR and Fusion SIEM:** Exabeam straddles the two market areas in its marketing and a lack of consistency across product naming and functionality has been an area of contention for end users.
- **Extended onboarding time:** The Exabeam SIEM requires a larger amount of professional services days to configure than other SaaS SIEMs in the marketplace. This adds cost and complexity for end users. Many professional services "bundles" are available.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. Its SIEM solution is FortiSIEM. It has a global footprint and customers in all major world regions, but especially North America and Europe. This product includes Advanced Agents (for Windows-based UEBA). FortiSIEM integrates with FortiSOAR, FortiAnalyzer and other elements of Fortinet's security product suite. Pricing is based on devices for SOAR, EPS and number of agents for SIEM. FortiSIEM is available as a virtual or physical appliance. Licensing is based on devices associated with 10 events per second per device. Perpetual and subscription licenses are available.

Strengths

- **Support for service providers and complex organizations:** Fortinet FortiSIEM offers built-in multitenancy support for complex organizations and service providers, as well as a variety of features specific to them. It also offers a consumption-based model for managed security service providers (MSSPs) with unlimited EPS.
- **Native asset visibility capabilities:** Fortinet FortiSIEM has powerful asset discovery and a built-in configuration management database (CMDB). This provides centralized visibility of assets discovered via active scanning and passive log inspection.
- **Integration with the wider Fortinet ecosystem:** Fortinet offers a diverse ecosystem of security and network products integrated via the Fortinet Security Fabric. Prospective and existing Fortinet clients looking for a single vendor to provide them with threat monitoring, detection and response solutions should consider Fortinet.

Cautions

- **Lack of a direct as-a-service strategy:** Fortinet relies on partners that offer hosting services for FortiSIEM as a means of delivering a SaaS-like experience to buyers. End-user organizations can deploy the solution in their own public or private cloud, or as a hybrid cloud model.
- **Limited coverage for monitoring cloud environments:** FortiSIEM's cloud security coverage is not as strong as that of other competitors. It lacks support for several public cloud infrastructure and platform services (CIPS), and the only cloud access security brokers (CASBs) supported are Fortinet's own FortiCASB product and Oracle CASB.
- **User and entity behavior analytics options:** UEBA is available in two flavors: a premium offering and a more limited version native to FortiSIEM. Both require agent deployment, and lack functions that are available from competitors, such as the ability to create dynamic peer groups. However, Fortinet's roadmap indicates that these gaps will be addressed.

Gurucul

Gurucul is a Visionary in this Magic Quadrant. Its SIEM is called Analytics-Driven SIEM and is a modular solution broadly focused on SIEM, UEBA, identity analytics, fraud analytics, SOAR and network traffic analysis. Gurucul offers a packaged TDIR capability via its Security Analytics and Operations Platform. The company's market presence is predominantly North American and its client profile is overwhelmingly based on large enterprise organizations. Gurucul has a robust roadmap extending into social media integration, security posture assessment integration, and improved integration with threat intelligence and digital risk protection services. Licensing is based on monitored assets and available as subscription or perpetual.

Strengths

- **Architecture and data lake support:** Gurucul supports a bring-your-own-data-lake and/or warehouse model preventing the need to replicate data in another data store for security. Gurucul offers a wide range of architecture options to support SaaS and client-deployable models.
- **Community machine learning models and threat content:** Open detections in Gurucul's threat detection library are available to all users for feedback and sharing, allowing for customization and sharing insights on variations of algorithms and threat content to modify detections.
- **Predictable pricing:** Gurucul prices its solution based on assets — which alleviates concerns about data volume or velocity overages — and there are no limitations on storage. It offers a modular structure allowing buyers to select only the features they need for their particular environment.

Cautions

- **Limited threat intelligence features:** Gurucul does not offer the same threat intelligence platform/management features as some competitors. Buyers needing threat intelligence functions (like link analysis, custom tagging and indicator management) will find these features lacking in Gurucul.
- **Market presence and execution:** Gurucul remains relatively unknown in the SIEM market despite increased marketing efforts. Buyers for SIEM are often unfamiliar with Gurucul or its solutions, and there is a lack of managed security services that support co-managed Gurucul deployments compared to other SIEM vendors.
- **Large environment focus:** The overwhelming majority of Gurucul clients are large enterprises, which often have the large and mature security teams needed to leverage a complex security SIEM like analytics-driven SIEM. Gurucul offers a multifaceted solution requiring more advanced data analytic and security operations experience.

Huawei

Huawei is a Niche Player in this Magic Quadrant. Its SIEM solution is called HiSec Insight and includes Huawei Cloud Security Brain. There are numerous additional modules and companion technologies for feature- or architecture-specific requirements. Its SIEM customers are largely concentrated in China; although a smaller number of clients are based in the Middle East, Africa and Latin America. Its customer base is split almost evenly between large and midsize enterprises, but there are also some smaller clients. Pricing for on-premises deployments is based on data velocity (EPS) and volume (gigabytes per day), with additional charges for log retention and add-on modules. SaaS deployments are based on the number of Elastic CloudServers purchased.

Strengths

- **Behavioral analytics:** Analytics has been an area of investment by Huawei. Its user behavior analytics provide dynamic peer-group-based detections. Its machine-learning-based risk ranking for entities reflects factors such as asset value, associated rule-based detections and vulnerability data.
- **Extensive product ecosystem:** Huawei offers a number of integrated capabilities, including network detection and response, sandboxing, deception, user behavior analysis, orchestration and response, and threat intelligence.
- **Flexibility in relation to form factors:** Huawei's product is available in multiple form factors that can be mixed as needed. These include software, physical and virtual appliances. There are also options for

hosting on Huawei's public or private cloud infrastructure.

Cautions

- **Limited support for cloud infrastructure monitoring:** Monitoring of cloud infrastructures is limited to Huawei's own cloud. No other cloud services are supported out of the box.
- **Lack of support for SaaS monitoring:** Out-of-the-box monitoring of popular SaaS applications is not provided. Huawei's platform lacks integrations with Microsoft 365, Google Workspace, or applications from Workday, Salesforce or Box.
- **Limited availability:** Huawei's focus on China, emerging markets in Asia/Pacific, and the Middle East and Africa means its product has little exposure to SIEM buyers elsewhere. Huawei has no immediate plans for expansion into North America or Europe.

IBM

IBM is a Leader in this Magic Quadrant. Its IBM QRadar product can be deployed via on-premises software, in a public/private cloud or hybrid, or delivered in a cloud-native format as QRadar on Cloud (QROC). IBM's SIEM customer base spans across North America, Europe, Asia/Pacific, the Middle East and Latin America, with the majority of them midsize and enterprise customers. In addition to QRadar, IBM offers other security products such as QRadar Network Insights, QRadar Vulnerability Manager, QRadar XDR Connect, QRadar SOAR (formally Resilient) and Cloud Pak for Security (CP4S). Licensing for QRadar SIEM is based on events per second (EPS) and/or flows per minute (FPM). Unlimited server-based licensing is an alternative option for cloud-deployed instances only.

Strengths

- **Strong analytics and customization:** QRadar has a large number of out-of-the-box content and analytic capabilities. Customers have also provided positive feedback around QRadar's ability to create and customize applications and dashboards.
- **Large security business and presence:** IBM has the global reach required (via direct and partner channels) to deliver its products, support and services in every major geographic region. In addition, it has ample staff members who understand region-specific regulations and speak multiple languages in order to support custom projects and configurations.
- **Multiple security product offerings:** IBM offers a broad range of optional, and tightly integrated add-on technologies, as well as services to complement and support QRadar. These include network security, vulnerability management, threat intelligence, data protection, UEBA, SOAR and MSSs/MDR services.

Cautions

- **Correlation rules and analytics are analogous:** QROC does not distinguish between correlation rules and analytics; hence, there are varying degrees of complexity, from simple to advanced, with regard to out-of-the-box content, which makes it hard to compare.
- **Cloud Pak slows SIEM innovation:** Innovation to QRadar SIEM has been slow as IBM shifts resources to the Cloud Pak for Security platform and next-generation security capabilities.

- **Implementations warrant improvement:** Based on feedback, clients have reported that the initial deployment can be a complex process. It may also lack flexibility in terms of onboarding new data sources.

Logpoint

Logpoint is a Niche player in this Magic Quadrant. Its SIEM solution is combined natively with SOAR functionality and is predominantly used by customers in a SaaS or cloud-based format. The largest concentration of buyers are small to midsize customers based in Europe. Logpoint has a notable offering for the monitoring and response of threats to SAP platforms. Licensing is based on the number of "nodes" monitored. The SOAR component is metered by the number of users, with a single-user license included with the SIEM product. UEBA capabilities are licensed separately.

Strengths

- **Simple, easy-to-understand pricing:** Logpoint offers a pricing model that is among the easiest to understand in the market. Tiered pricing based on the number of "nodes" (or assets) sending logs to the solution is available for the core SIEM element of the product, with the bundled SOAR priced by the number of users (a single-user license is included with the SIEM product).
- **Third-party SaaS application monitoring:** An emphasis on third-party SaaS platforms is clearly part of Logpoint's strategy, with significant capabilities for SAP and Salesforce, and good support for Microsoft 365. Integrations for Amazon's S3 service and ServiceNow are also available.
- **Services support:** Logpoint's SIEM + SOAR offering has complementary available service offerings to support operational monitoring of the SIEM and design and development of SOAR playbooks. These are available at an extra subscription cost directly from Logpoint.

Cautions

- **Lack of UEBA self-build functionality:** Logpoint supports a number of tool sets that have the ability to deliver analytics content, and although a large number of out-of-the-box analytics are available, advanced users will not be able to create new user and entity behavioral analytics for themselves.
- **Singular SaaS SIEM storage pricing model:** Logpoint includes 90 days of indexed log storage with its SaaS product. A further 90 days of "cold" storage is chargeable, and buyers that require longer periods of storage must purchase in 90 day increments. Potential buyers should inquire about the cost of longer-term storage. Offloading to third-party log storage is available.
- **Europe-centric:** Logpoint predominantly serves customers in one region, Europe. Sales are evident in North America, and infrastructure and sales forces appear to be present in the region and are growing. Buyers should satisfy themselves that the level of international support they require is available.

LogRhythm

LogRhythm is a Challenger in this Magic Quadrant. Its SIEM solution is the LogRhythm SIEM Platform, which includes several add-on components to deliver endpoint, network and user-behavior analytics. A large majority of its SIEM customers are in North America and Europe, with the rest in Asia/Pacific, the Middle East, Africa and Latin America. Its customer base is skewed toward midsize enterprises and smaller organizations, though large enterprises have also purchased the LogRhythm SIEM. There is a cloud option

available, but most customers have deployed its SIEM on-premises. Licensing is available on a perpetual basis (priced by average number of messages per second, per day) or a subscription basis (priced by number of employees).

Strengths

- **Extensive resellers:** LogRhythm has a strong team of reseller partners in every major world region. This strength is mirrored by broad support from managed service providers to help modestly resourced buyers manage and monitor its SIEM.
- **Pilot and proof of concept (POC) options:** Buyers can take advantage of several types of pilot and POC program, ranging from prepilot workshops, to hosted, scenario-based test-drive exercises and "try and buy" options.
- **Investigation and case management workflow:** LogRhythm provides mature and refined investigation and case management capabilities that assemble context and enable users to create an evidence base for case disposition.

Cautions

- **Limited cloud-based options:** LogRhythm's recent acquisitions and product roadmap demonstrate progress in early development of its SaaS SIEM capabilities, but the vendor lags behind many competitors in this regard. The cloud SIEM offering delivers split interfaces requiring users to switch between two environments. The administrative functions use the legacy LogRhythm administration console to create parsers and rules, and to manage threat intelligence feeds. The dashboard and alerts UI is more aligned to what users would identify as cloud-native.
- **App store is challenging:** LogRhythms app store is offered within the legacy admin console application Knowledge Base. It has only basic features and does not look like a modern SaaS app store, where users can utilize API key integrations to easily onboard point solutions or data sources (as is the case with competing solutions).
- **Move to the cloud:** LogRhythm faces the challenge of developing a new cloud-based SIEM and introducing its capabilities to buyers, while at the same time maintaining its legacy SIEM and executing its plans to migrate customers to the new SaaS architecture.

ManageEngine

ManageEngine is a Niche player in this Magic Quadrant. Its Log360 SIEM solution is cloud-based and deployed in the Zoho Corporation's own data center. The predominant buyers of Log360 are midsize and enterprise customers primarily across the North America, Europe, Middle East and Asia/Pacific regions. In addition to its SIEM tool, Log360 includes other security products such as Firewall Analyzer, EventlLog Analyzer, ADAudit Plus, Vulnerability Manager Plus, Cloud Security Plus, DataSecurity Plus and FileAnalysis. Licensing for SaaS is based on the amount of data stored in the cloud over a specific period. The on-premises version's licensing is based on the number of log sources. This includes devices such as workstations, Windows servers and other network devices. Capabilities like user and entity behavior analytics (UEBA), advanced threat analytics, and application auditing are available as add-ons.

Strengths

- **Cloud security capabilities:** ManageEngine now offers CASB capabilities, which can be accessed through Log360 Cloud. This provides enrichment to the Log360 SIEM solution, as well as the ability to detect unauthorized cloud applications and stop the use of any banned applications.
- **Ease of implementation and operations:** Reviews on Gartner's Peer Insights around ManageEngine's ability to easily deploy and use the SIEM tool are generally positive.
- **Native data privacy and protection features:** ManageEngine provides data encryption, masking and obfuscation capabilities, which align to the General Data Protection Regulation (GDPR) privacy and data protection requirements.

Cautions

- **Lacks advanced capabilities:** ManageEngine lacks more advanced capabilities that would most likely be needed and required by more mature organizations, such as advanced analytics (supervised ML and deep learning analytics, for example) and native SOAR.
- **Limited integrations with third-party solutions:** ManageEngine's Log360 product has limited bidirectional integrations with third-party security tools, such as EDR, NDR and SOAR.
- **User interface limitations:** Although Log360 supports integrations with leading ITSM tools, and has its own chat feature, it does not display information from third-party systems, nor can it share content (such as reports) between users.

Micro Focus

Micro Focus is a Visionary in this Magic Quadrant. Its ArcSight product is mainly focused on SIEM, UEBA, SOAR and TIP functionality. ArcSight's operations are geographically diversified (with the exception of Latin America) and its client profile is predominantly midsize. On-premises deployments far outweigh cloud-native deployments, largely attributed to recent availability of its cloud option. Micro Focus has invested heavily in its CyberRes portfolio of security products that includes data security, identity access management (IAM), application security and security operations. The first major product focus from the CyberRes security operations portfolio is Galaxy, a cloud-native threat intelligence solution that integrates into the ArcSight workflow. Licensing is based on EPS for SIEM and per entity for UEBA.

Strengths

- **Threat intelligence platform (TIP):** The Galaxy Threat Acceleration Plus (GTAP) Basic TIP solution is included with ArcSight SIEM. It provides MISP open-source intelligence to all ArcSight buyers at no additional cost, and can be upgraded to GTAP Plus, which provides CyberRes premium threat intelligence feeds. This SaaS TIP solution provides a graphical view and link analysis between indicators.
- **SOAR included with SIEM:** ArcSight SIEM includes SOAR at no additional charge but it is not a SaaS-based feature as yet. Users can use a graphical canvas to create workflows with a plethora of configuration options presented as drop-downs. Automation engineers can also use a code-based development interface for more complex playbook creation. All automated response actions are recorded in a case management file.
- **ArcSight Fusion UI:** The Fusion UI provides an updated interface with a SaaS feel, indicating a departure from the historical ArcSight console UI. Fusion provides modern timelining and graphical views of data to

show patterns of activity for a user or entity. Analysts can use a slider to filter events based on risk to narrow the activity in an investigation.

Cautions

- **Split UI between ArcSight Console and SaaS:** Users will find there is still a need to turn to the functional but older ArcSight Console UI for management functionality, even in the SaaS architecture. FlexConnector, Quick Flex, FlexAgent, Correlation Condition Editor (CCE) are all examples where the older ArcSight console is still required versus use of the updated Fusion UI.
- **Analytics customization/creation requires external tools:** ArcSight does not provide a UI for custom machine learning model support. Instead, users leverage third-party data science tools (such as SPSS, SAS or R) to export models in a standard PMML format. These models can then be imported into ArcSight. While this removes the burden of needing to learn an ArcSight-specific analytics UI and workflow, leveraging external tools may not be quite as intuitive or user friendly to some buyers.
- **Associated event view options:** Micro Focus only demonstrated two options for viewing events that are associated with a discovered incident in ArcSight. The primary method is through ArcSight's native incident management (SOAR) interface, and the second method is via PDF download. Some buyers may desire additional options to aid in investigative workflows. Buyers will have to engage with Micro Focus for additional guidance and options.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its SIEM product, Microsoft Sentinel, is delivered only as SaaS via Microsoft's Azure data centers. Microsoft has a large and diverse customer base, catering for large and small customers alike, and offering the SIEM product in multiple settings internationally. Licensing is based on the volume of data ingested, via reserved capacity, or pay-as-you-go. However, many of the Microsoft enterprise tiers for Microsoft 365 include credit for Sentinel and Defender usage. Enhanced data storage, complementary Microsoft ecosystem capabilities (such as Defender for Endpoint and Defender for IoT) are available at extra cost.

Strengths

- **Rich ecosystem of highly integrated security products:** Microsoft inherently provides a large number of highly integrated ecosystem products in areas such as CASB, identity, endpoint, network and OT security. Furthermore, a number of its traditional IT capabilities have bidirectional integrations. Buyers that invest in a wide set of Microsoft products — both security and nonsecurity — can expect excellent security visibility across their estate.
- **Fast-developing roadmap:** Clients that are investing in Microsoft Sentinel have already seen a significant and continued increase in functionality, usability and growth in end-user communities over the period of their investment.
- **Tiered and hybrid operations:** The ability to consistently configure, manage and oversee several conjoined Sentinel instances using the "Lighthouse" functionality benefits both users with complex environments, and those who are using Sentinel and want to move to a managed services model with either Microsoft directly or with one of the growing number of managed services partners in the marketplace.

Cautions

- **Difficult to understand the true cost:** Although pricing uses a simple data ingestion model for pricing, and has pay-as-you-go options, clients report that pricing is unpredictable and complex to understand when combined with other Microsoft licensing. Buyers considering Sentinel should take into account the cost of moving data from their on-premises and third-party cloud assets alongside the pricing for the SIEM.
- **Potential for indirect vendor lock in:** Integrating Microsoft products into Sentinel is easy to implement, however, it is difficult to compare native Microsoft functionality and pricing with third-party integrations. Buyers should plan their SOC tool selections carefully and ensure that their dependence on any one vendor does not impact their ability to deliver against their objectives.
- **Limited out-of-the-box content:** When compared with many of the other SIEM products, Sentinel is missing some out-of-the-box features, including compliance reporting. However, clients have the flexibility to create their own analytical content, which is less common across the market space. Buyers should consider the additional expense of professional services required to support the delivery of their needs when evaluating the true cost.

Rapid7

Rapid7 is a Challenger in this Magic Quadrant. Its SIEM solution, InsightIDR, runs on the cloud-based Insight platform. Other products available include InsightVM (vulnerability management), InsightAppSec, InsightConnect (SOAR), InsightCloudSec (cloud security posture management) and Threat Command (threat intelligence). Customers of the InsightIDR SIEM are concentrated most heavily in the U.S., followed by Europe and APAC. Licensing is based on a term license, with a straightforward pricing model based on the number of assets monitored.

Strengths

- **Wide range of integrated capabilities:** Rapid7 offers a core SIEM with a multitude of security capabilities, including InsightVM, which offers vulnerability management; and InsightIDR, which has capabilities in EDR, UEBA and NDR. All of these capabilities are highly integrated with one another for a single experience for SOC operators.
- **Cost-effective:** Rapid7 is among the most cost-effective solutions evaluated as part of this research, with an average price for its core SaaS SIEM far lower than the market average.
- **Managed detection and response service:** This is available directly from Rapid7 at additional cost. It represents a single source for customers that want access to the SIEM product and need service support for monitoring and investigation.

Cautions

- **No compatibility with third-party data storage:** Rapid7's SIEM product has little or no support for recalling data from third-party storage. This may lead to added cost and increased regulatory needs. Buyers with large-ranging storage requirements — or specific needs around regional data residency — should ensure that Rapid7 can meet their requirements in these areas.
- **Maintenance of third-party automation integrations:** Rapid7 has no commercially available integrations for third-party SOAR/automation platforms. Buyers who have already invested in these tools should consider the maintenance overhead of integrating or using the products together as part of their security operations technology set.

- **Lack of support for data obfuscation:** Rapid7's solution is unable to support data obfuscation natively which means that data stored in the platform may not be able to meet some privacy standards or localized compliance requirements. Buyer should engage with Rapid7's professional services teams — or possibly third-party solutions — if they have a requirement to obfuscate log data.

Securonix

Securonix is a Leader in this Magic Quadrant. Its SIEM solution is Next-Gen SIEM and includes Next-Gen SIEM, Security Data Lake, UEBA, SOAR, NDR, threat intelligence, adversary behavior analytics and several use-case-specific applications (such as for healthcare and SAP). Most Securonix customers are in North America, followed by Europe, Asia/Pacific, the Middle East and Africa, and Latin America. Customers are mostly large enterprises, but its products also appeal to some midsize customers. Smaller customers are mostly served by managed service partners. Licensing is based on identities and EPS. Most buyers opt for term licenses, but perpetual licenses are available.

Strengths

- **Third-party data lake access:** Securonix SIEM is able to query and display live data from third-party systems such as data lakes, enabling the platform to operate in a more decentralized fashion. Data decentralization enables more cost-effective deployments, with more up-to-date data, and is expected to be a key trend for SIEM over the next 18 months.
- **Threat intelligence access included:** Securonix provides a set of threat intelligence integrations for additional enrichment at no additional charge. It has published this information into the public domain for use.
- **Investigation and case management workflow:** Securonix provides refined investigation and case management capabilities that assemble context and share with context and collaboration within the platform.

Cautions

- **Overlap in Open XDR and Next-Gen SIEM marketing messaging:** Securonix straddles the two market areas in its marketing, so make sure you understand what you need from the product when purchasing.
- **Unconventional pricing models:** Securonix uses a model that considers both EPS and identities. Users should evaluate EPS requirements to avoid unexpected increase in cost. Users may experience inconsistency and unpredictability in required event rates, and therefore cost.
- **Additional Analytics packaging:** Securonix has a complex set of premium analytics apps that are priced per-user, per-app. When evaluating, you need to understand which analytics app's capabilities are already included, or need to be added for correct evaluation. While the cost of buying all functionality is similar to a single analytics add-on from other SIEM vendors, it is difficult to compare offerings, contrast with the market, and plan what capabilities are required.

Splunk

Splunk is a Leader in this Magic Quadrant. Its SIEM is Enterprise Security (Splunk ES) and is an add-on to the Splunk Enterprise solution. It is important to note that Gartner does not assess or view the core Splunk Enterprise solution as an SIEM. The majority of Splunk ES buyers are based in North America. The predominant buyers of Splunk ES are large enterprise organizations. The direction of Splunk ES is to offer

more enrichment of events and artifacts through its UI, and promote more content delivery. Licensing is available as volume per day or cloud workloads (referred to as “Splunk Virtual Compute”).

Strengths

- **Packaged security features:** The SaaS model of Splunk ES includes TIP and UEBA capabilities at no additional cost. Historically, Splunk has used a modular product model to sell its offerings, but is now packaging critical components with Splunk ES to deliver a more comprehensive security solution.
- **IT observability coupled with security:** A continuing advantage for Splunk is its ability to deliver IT observability and analytics to nonsecurity users, while providing joined security operations functionality via Splunk ES to security teams. Splunk is increasing the fusion of environmental data with security to provide users with an enriched view of its environment.
- **Security operation user experience:** Buyers of Splunk consistently report positive user experience with the ES product via power query functionality, API capabilities, customized dashboards and data-science-based analytics provided out of the box.

Cautions

- **Pricing:** Buyers are still reporting angst with Splunk costs and the newer Splunk Virtual Compute (SVC) pricing has not provided the relief promised. Increasing demands to log everything are forcing existing Splunk clients and new buyers alike to look at cheaper alternatives to offset massive data ingestion and storage costs.
- **Complexity and expertise:** Buyers express trepidation about the complexity of Splunk ES and existing users communicate problems with data management within the solution. There are also real issues with training, keeping and hiring Splunk ES expertise in the market due to the high-demand competitiveness between owners of Splunk ES for the finite talent pool.
- **Regional sales expertise:** The majority of Splunk’s salesforce is based in North America, with a smaller undisclosed percentage outside the region. Lack of understanding of local market requirements and restrictions can lead to poor experience from a sales and support perspective.

Sumo Logic

Sumo Logic is a Visionary in this Magic Quadrant. Its SIEM product, Cloud SIEM, is delivered as a SaaS-only solution. Sumo Logic’s customer base is an equal mix of small, midsize and enterprise customers, with the majority based in North America. The company has increased its presence in the Europe and Asia/Pacific regions over the past year. In 2021, Sumo Logic acquired DFLabs, which provides additional incident handling processes, automated playbook actions, and enrichment via external information sources with a similar efficacy to a stand-alone SOAR offering. Licensing is subscription-based (with pricing based on data ingestion) or credit-based (with credits being used to enable specific resource usage, such as for occasional search or continuous analytics), with tiering and packaging options.

Strengths

- **SecOps and DevOps unification:** Sumo Logic’s uses can extend beyond security operations use cases into development and operations, which is the company’s heritage, and democratizes the data for multiple business units.

- **Free commercial off-the-shelf TI:** Sumo Logic provides threat intelligence via CrowdStrike for additional enrichment at no added charge.
- **Integrated SOAR functionality:** DFLabs SOAR capabilities are now assimilated into the SIEM post-acquisition, which reduces time-consuming SecOps tasks as well as the time needed to deploy an SOAR and then do the integration work to make it functional.

Cautions

- **Advanced analytics:** Sumo Logic does not have the breadth of advanced analytics capabilities, such as UEBA, when compared to other SIEM competitors in the market.
- **Searching experience:** Reviewers on Gartner's Peer Insights have expressed concerns around Sumo Logic's searching capabilities, specifically impacting performance when searching for large sets and/or older data.
- **Limited visibility:** Although Sumo Logic has increased visibility across MSSPs/MDR providers in terms of resellers and/or managed SIEM support, its mind share for SIEM among end-user Gartner clients remains low.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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.

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant 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

- Devo met the commercial and functional requirements for inclusion in the 2022 Magic Quadrant for SIEM.

Dropped

- VenusTech did not meet functional and commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM.
- FireEye combined with McAfee via acquisition to form Trellix and did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM.
- McAfee combined with FireEye via acquisition to form Trellix and did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM.
- Odyssey did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM.

- Netwitness, an RSA company, did not meet functional and commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts considered necessary for a vendor to be included in this Magic Quadrant.

To qualify for inclusion, a vendor needed to fulfill the following criteria:

- A product that provides SIM and SEM capability to end-user customers via cloud-native software and/or SaaS.
- Features, functionality and add-on solutions including at least two of the below named additional capabilities that were generally available, vendor-owned (wholly acquired or organically built) and included in the SIEM product or sold as separate add-ons as of 1 February 2022.
  - Security orchestration, automation and response (SOAR)
  - Threat intelligence platform (TIP)
  - User and entity behavior analytics (UEBA)
  - Long-term data storage and reporting (greater than 365 days)
- A product that supports data capture and analysis from heterogeneous, third-party sources via API in addition to data streaming or log collection (that is, other than from the SIEM vendor's products/SaaS), including market-leading network technologies, endpoints/servers, cloud (IaaS or SaaS), and business applications. This must include bidirectional, formally recognized partnerships with at least 10 major security technology vendors.
- Cloud-native/SaaS license and maintenance (excluding managed services) revenue exceeding $50 million for the 12 months prior to 1 February 2022, or have 100 distinct production customers with direct contracts on cloud-native or SaaS platforms as of the end of that same period.
- In the 12 months prior to 1 February 2022; to have received 15% of SIEM cloud-native/SaaS revenue from buyers with headquarters outside the geographical region of the vendor's headquarters location, or having at least 20 production customers, each with headquarters outside the geographical region of the vendor's headquarters location.
- Sales and marketing operations (via print/email campaigns, local language translations for sales/marketing materials) promoting SIEM products targeting at least two geographical regions as of 1 February 2022.

Excluded from consideration were:

- Capabilities available only through a managed services relationship — that is, SIEM functionality available to customers only when they sign up for a vendor's managed security, or managed detection and response, or managed SIEM, or other managed services offering. By managed services, we mean those in

which the customer engages the vendor to establish, monitor, escalate and/or respond to alerts, incidents and cases.

Honorable Mentions

- **DataDog** was not surveyed as part of this Magic Quadrant process, however it is considered alongside SIEM products by Gartner clients due to its cloud native architecture, log processing capabilities and visualizations. DataDog also operates a freemium version of its product, including infrastructure monitoring functions. Datadog is a consideration for buyers who are focused on log collection and human-driven analysis.
- **Graylog** did not meet the functional requirements for inclusion in this Magic Quadrant. Graylog is another SIEM vendor that started with providing infrastructure and application monitoring, and then began offering support for security operations use cases. It now offers Graylog Security, which includes prepackaged SIEM and UEBA content out of the box under one license.
- **Logsign** did not meet the commercial requirements for inclusion in this Magic Quadrant. Logsign will appeal to buyers familiar with Elastic search. It offers a combination of SOAR and SIEM capabilities built around a streamlined user interface with customizable dashboards.
- **Google Chronicle** was not surveyed as part of this Magic Quadrant. Chronicle has an obvious native advantage for organizations with a large Google Cloud presence, and integrates with Google Security Command Center. Chronicle is capable of large-scale log ingest, and offers fast search capabilities. As a result of the acquisition of Siemplify, Chronicle can now be coupled with SOAR functionality.
- **Panther Labs** did not meet the commercial requirements for inclusion in this Magic Quadrant. It offers a cloud-native detection-as-code platform as a SIEM alternative for cloud-focused threat detection, and can support AWS and Snowflake data warehouses. Panther Labs also offers a serverless architecture and is fully managed by its support team.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion evaluates a vendor's ability to provide product functions in core SIEM areas such as the ability to create, modify and maintain threat detection use cases, provide case management and support incident response activities and generate reports to support business, compliance and audit needs.

Overall Viability: This criterion includes an assessment of a vendor's customer traction, the financial and practical success of its SaaS SIEM business, and indicators that it will continue to invest in SIEM technology.

Sales Execution/Pricing: This criterion evaluates a vendor's success in the SIEM market and its capabilities in presales activities. Considerations include the size of its SIEM revenue and installed base for its cloud-native/SaaS SIEM revenue and installed base, flexibility of pricing models, its presales support, and the distribution and inclusivity of its sales channel. The level of interest and reviewed experiences from Gartner clients is also considered.

Market Responsiveness/Record: This criterion evaluates the delivered features and alignment to client demand for adjacent SIEM capabilities and modern deployment methods as well as the track record of

delivering new and differentiated functions in line with the changing needs of the market. Considerations include support for multicloud monitoring, cloud-native or SaaS business focus, and industry-specific support within areas such as OT.

Marketing Execution: This criterion evaluates a vendor's SIEM market messaging in light of Gartner's understanding of customer needs. It also identifies particular vendor-identified variations by industry or geographic segment.

Customer Experience: This criterion evaluates product function and service experience in production environments. Included are, operations, administration, and vendor support capabilities. This criterion assesses areas such as, available support and training, customization of user interfaces, and takes into account interactions with Gartner clients that are using, or have completed competitive evaluations of, a vendor's SIEM offering.

Operations: This criterion evaluates a vendor's service, support and sales capabilities. It includes an assessment of these capabilities across multiple geographies.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Medium

Source: Gartner (October 2022)

Completeness of Vision

Market Understanding: This criterion evaluates a vendor's ability to understand buyers' emerging needs and how to communicate solutions effectively. SIEM vendors that show the highest degree of market understanding can identify how technology and changes in ways of working will translate into modern security operations requirements, while also meeting the business risk and ROI reporting needs of organizations.

Marketing Strategy: This criterion evaluates a vendor's ability to communicate the value and competitive differentiation of its SIEM offering.

Sales Strategy: This criterion evaluates a vendor's use of direct and indirect sales, marketing, service, and communications affiliates to extend the scope and depth of its market reach.

Offering (Product) Strategy: This criterion evaluates a vendor's approach to product development and delivery, with an emphasis on how well functionalities and features correspond to current requirements. Development plans during the next 12 to 18 months are also evaluated. 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. We assign higher weightings to coverage of emerging event sources, such as IaaS and SaaS, and environmental context.

Business Model: Despite vendors' focus on expanding their capabilities, we continue to value speed and simplicity of deployment and breadth of platform support. Users, especially those with limited IT and security resources, still value this attribute over breadth of coverage beyond basic use cases. SIEM products are complex and tend to become more so as vendors extend their capabilities. Vendors able to provide effective products that users can successfully use as a service — or deploy, configure and manage with limited resources — will be the most successful. We evaluate options for co-managed or hybrid deployments of SIEM technology and supporting services, because growing numbers of Gartner clients are anticipating or requesting vendor-delivered service wrappers (VDSW) or security service provider partner support for monitoring or managing their SIEM technology deployments.

Vertical/Industry Strategy: This criterion evaluates a vendor's strategy to support SIEM requirements specific to industries, like operational technology (OT) environments.

Innovation: This criterion evaluates a vendor's development and delivery of SIEM technology that is differentiated from that of its competitors in a way that uniquely meets customers' most important requirements. Product capabilities and customer use in areas such as application layer monitoring, identity-oriented monitoring and incident investigation are evaluated. This is in addition to other product-specific capabilities that are needed and deployed by customers. Heavy weightings are assigned to capabilities needed for advanced threat detection and incident response: user, data and application monitoring; ad hoc queries; visualization; orchestration and incorporation of context to investigate incidents; and workflow/case management features.

Geographic Strategy: This criterion takes account of the fact that, although the North American and EMEA markets produce the most SIEM revenue, Latin America and Asia/Pacific are growth markets for SIEM, and their growth is driven primarily by demand for threat management (and secondarily by compliance requirements). Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of their sales and support strategies for those regions, as well as product features to support local and regional compliance requirements for data residency and privacy.

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	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2022)

Quadrant Descriptions

Leaders

Leaders provide products that are a strong functional match for the market's general requirements. These vendors have been the most successful at building an installed base and revenue stream in the SIEM market. In addition to providing technology that is a good match for current customer requirements, Leaders show evidence of superior vision and execution for emerging and anticipated requirements. They typically have a relatively high market share and/or strong revenue growth, and receive positive customer feedback about their SIEM capabilities and related service and support.

Challengers

Challengers have multiple product and/or service lines, at least a modestly sized SIEM customer base, and products that meet a subset of the market's general requirements. Challengers typically have strong execution capabilities, as evidenced by financial resources and a significant sales and brand presence. However, Challengers either do not demonstrate a complete set of SIEM capabilities or lack a track record of competitive success with SIEM technologies comparable to the track records of Leaders.

Visionaries

Visionaries provide products that are a strong functional match for the SIEM market's general requirements, but have less Ability to Execute than Leaders. Their lower Ability to Execute is typically due to lower scores for product features and functions, or to a smaller presence in the SIEM market than that of the Leaders. This is measured by installed base, revenue size or growth, overall company size or general viability (or a combination of these attributes).

Niche Players

Niche Players are primarily vendors that provide SIEM technology that is a good match for a specific SIEM use case or a subset of the SIEM market's functional requirements. Niche Players focus on a particular segment of the client base (such as midsize organizations, service providers, or a specific region or industry) or may provide a limited set of SIEM capabilities. In addition, Niche Players may have a small installed base or be limited, according to Gartner's criteria, by other factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broad set of capabilities to organizations now and during a 12-month planning period. Inclusion in this quadrant does not reflect negatively on a vendor's value for narrowly focused markets or use cases.

Context

The SIEM market continues to add more functionality and shift architecture strategies to meet client demands. This Magic Quadrant places emphasis on global SaaS architecture availability and multifaceted platform features like SOAR, UEBA, TIP, self-serve analytic creation, continuous threat content creation and incident management features. Organizations continuing to seek self-deployed and managed architectures will increasingly find their options limited as more SIEM vendors move to either predominate or exclusive SaaS architecture offerings.

Readers should leverage this Magic Quadrant research as one of many resources to aid in their buying decision, not as the single source of truth. Readers should not infer that a vendor in the Leaders quadrant is by default the best choice for their particular use case or environment. Assess vendors against individual business and security needs, not where they are placed in the quadrant.

This research assesses vendors based on their solutions as offered in 2021 up to 1 February 2022, to include the strength of their SIEM product roadmaps. The SIEM market is continuously evolving meaning this research is a point in time assessment. As such, readers should leverage the companion Critical Capabilities for Security Information and Event Management, which may include off-cycle updates throughout the year as vendors make significant changes that warrant a Critical Capabilities scoring update.

Market Overview

The SIEM market grew from $3.41 billion in 2020 to $4.10 billion in 2021 (see Market Share: All Software Markets, Worldwide, 2021), a 20% annual growth rate compared to a 3.9% decline the previous year. The primary drivers of a SIEM purchase are threat detection, response, exposure management and compliance. Buyers are seeking a SIEM ecosystem with broad and deep capabilities to satisfy multiple security and business use cases with capabilities to support a diverse environment.

The SIEM market is maturing at a rapid pace and continues to be extremely competitive. The reality of what SIEM was just five years ago is starting to detach from what SIEM is and provides today.

SIEM is now widely supporting exposure management capabilities by leveraging data points such as configuration status of cloud assets, risk profiling across users and entities, asset inventory and criticality rating, with the purpose of delivering a real time risk posture. This combination of use cases helps security and risk management (SRM) leaders build a compelling business case for purchasing based on outcome-delivered metrics (see Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security), which can answer questions from the business about what value a SIEM will deliver rather than focusing on how much it costs.

The SIEM market has been moving toward a feature-rich security solution to offer clients numerous options to address their security needs, such as:

Threat detection:

- Real-time analytics
- Batch analytics
- Data science algorithms
- User- and entity-based analytics

Response:

- SOAR
- Incident management
- Collaboration

Exposure management:

- Asset details (criticality, grouping, location, patch status, etc.)
- User details (criticality, peer grouping, business unit, role, incident history, etc.)
- Configuration posture (cloud asset configuration, GPO settings, etc.)
- Poly-cloud visibility and unified exposure understanding
- Threat detection framework alignment

Compliance:

- Reporting
- Continuous monitoring requirements
- Audits
- Security system of record

The most prominent deployment architecture has shifted from client-hosted and managed, to cloud-native (SaaS) or cloud-delivered (hosted) to take advantage of easier deployments, scalability and flexibility. SaaS options reduce buyer requirements to manage and maintain a SIEM deployment allowing them to focus on security outcomes, versus patching and upgrading SIEM hardware and software versions. This shift to SaaS has enticed small and midsize organizations to invest in SIEM to have custody of their security data, and the current market growth supports this. In turn, we have observed an increase in co-managed SIEM services to deliver full-time SOC monitoring and optimization of client-owned SIEM solutions. There are markets where on-premises/hosted architectures remain a requirement (for now) and SIEM vendors need to continue to expand support in regional cloud provider data centers. Data sovereignty and privacy laws will continue to impact data residency and access, which SIEM vendors can address by deploying their solutions regionally, and restrict data residency based on buyer requirements.

The SIEM market will continue to evolve and see increased competition with new solutions that have come to market. Extended detection and response (XDR) is targeted at organizations with a less mature security operations posture, or that lack the ability to run a complex SIEM solution. These buyers are prone to buying vendor delivered service wrappers (VDSW) from their technology vendor of choice to run the security solution they have purchased due to lack of resources.

SIEM vendors have already begun to invest in (or acquire) telemetry collection solutions to deliver a prebuilt ecosystem of security technologies for buyers who are looking for an encapsulated security solution. One that delivers threat detection, security log retention, compliance reporting, behavioral analytics, automation, investigation and response actions. SIEM, UEBA, SOAR, TIP, EDR, NDR and cloud security solutions in a packaged offering are already on the market, and the expectation is that this trend will continue to grow. This aligns to the concept of the cybersecurity mesh and a composable security architecture. However, it is unrealistic to expect that every organization will want a single vendor to provide its entire security stack, which will allow the vendor choice option to persist well into the future.

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 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.

Stratégie géographique : la stratégie du fournisseur pour orienter les ressources, les compétences et les offres afin de répondre aux besoins spécifiques des zones géographiques en dehors de la zone géographique "d'origine" ou d'origine, soit directement, soit par l'intermédiaire de partenaires, de canaux et de filiales, selon les besoins de cette zone géographique et de ce marché.