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

8 mai 2024 - ID G00780705 - 54 minutes de lecture

Par **et 2 de plus** Andrew Davies , Mitchell Schneider ,

SIEM a évolué vers une plate-forme de sécurité dotée de plusieurs fonctionnalités et modèles de déploiement pour fournir un système de sécurité d'enregistrement doté de capacités complètes de détection, d'enquête et de réponse aux menaces. Cette recherche aide les responsables de la sécurité et de la gestion des risques à évaluer les fournisseurs dans cet espace.

Définition/description du marché

Ce document a été révisé le 9 mai 2024. Le document que vous consultez est la version corrigée. Pour plus d'informations, consultez la page **Corrections** sur gartner.com.

SIEM est un système de sécurité configurable qui regroupe et analyse les données d'événements de sécurité provenant d'environnements sur site et cloud. SIEM participe aux actions de réponse visant à atténuer les problèmes qui nuisent à l'organisation et à satisfaire aux exigences de conformité et de reporting.

Le système de gestion des informations et des événements de sécurité (SIEM) doit contribuer à :

- Agrégation et normalisation des données provenant de divers environnements informatiques et de technologies opérationnelles (OT)
- Identifier et enquêter sur les événements de sécurité d'intérêt
- Prise en charge des actions de réponse manuelles et automatisées
- Maintenir et rendre compte des événements de sécurité actuels et historiques

Capacités indispensables

Les capacités indispensables pour ce marché comprennent :

- Collecte de détails d'infrastructure et de données pertinentes pour la sécurité à partir d'un large éventail d'actifs situés sur site et/ou dans une infrastructure cloud.

- Possibilité pour les utilisateurs finaux d'auto-développer, de modifier et de maintenir des cas d'utilisation de détection des menaces à l'aide de méthodes basées sur la corrélation, l'analyse et les signatures .
- Fournir le contenu du fournisseur SIEM et les installations pour le contenu créé par le client , dans des domaines tels que : l'analyse, la normalisation des données, la collecte et l'enrichissement.
- Fourniture de gestion de cas et de soutien aux activités de réponse aux incidents.
- Générations de rapports pour répondre aux besoins commerciaux, de conformité et d'audit, selon les besoins.

Capacités standards

Les capacités standard pour ce marché comprennent :

- Stockage des données essentielles sur les événements de sécurité à long terme et mise à disposition pour la recherche
- Permettre la collecte de données d'événements provenant de sources d'événements disparates, à l'aide de plusieurs mécanismes (flux de journaux, API, traitement de fichiers) à des fins de cas d'utilisation de détection de menaces, de reporting et d'enquête sur les incidents.
- Plusieurs options de déploiement pour inclure sur site, hébergé dans le cloud, cloud natif ou SaaS
- Données de normalisation, d'enrichissement et de score de risque provenant de systèmes tiers
- Orchestration et automatisation des tâches et des workflows pour améliorer les enquêtes et limiter l'impact des incidents
- Fonctionnalité SOAR (Security Orchestration Automation Response) complète
- Capacités d'analyse avancées utilisant l'analyse du comportement des entités utilisateur (UEBA) et les sciences des données (c.-à-d. apprentissage automatique supervisé et non supervisé, apprentissage profond/réseaux neuronaux récurrents)
- Capacités de la plateforme de renseignement sur les menaces (TIP) pour gérer les renseignements et fournir des informations contextuelles sur les menaces

Capacités facultatives

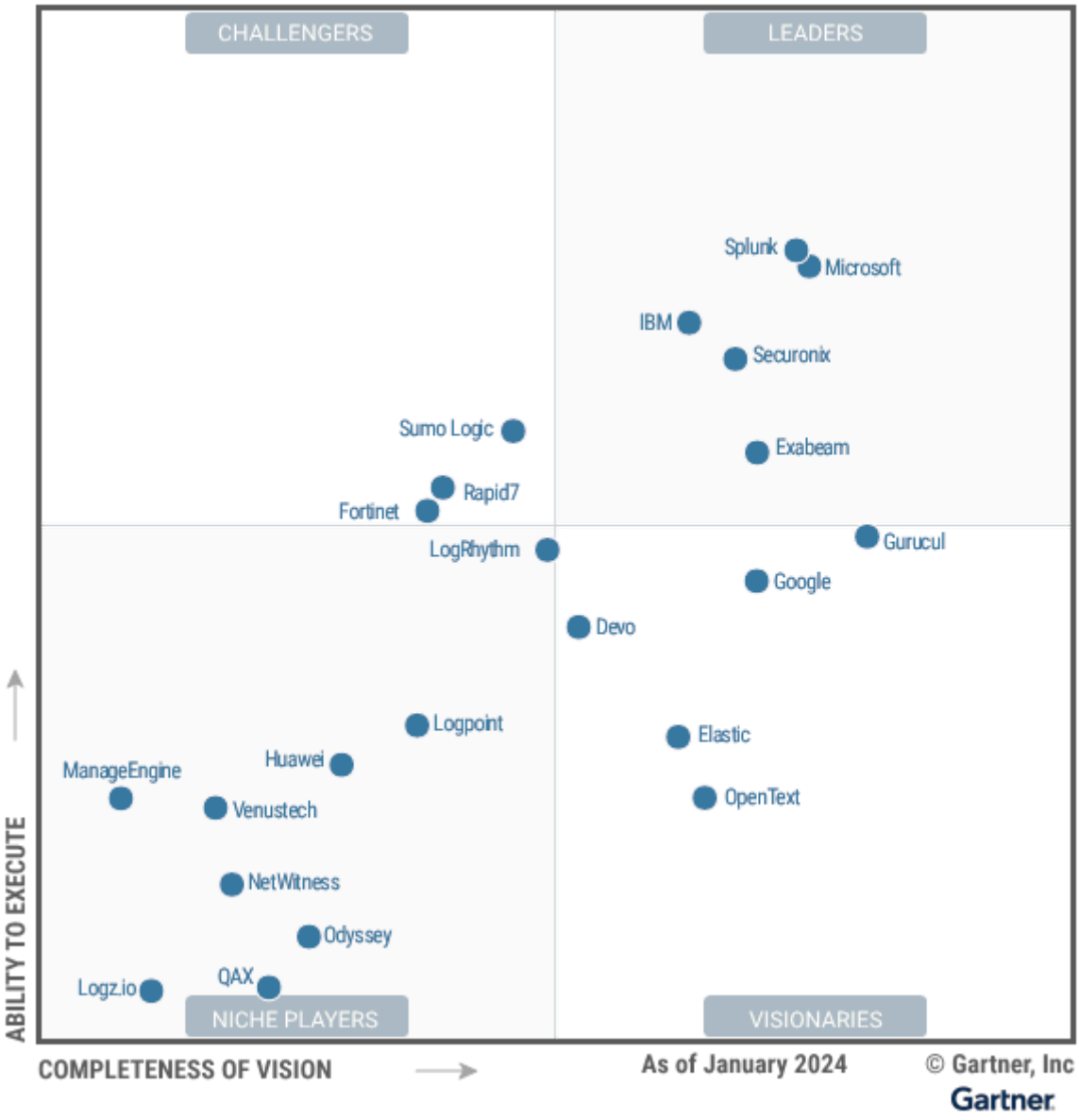
Les capacités optionnelles pour ce marché incluent :

- Plateformes permettant aux clients de s'abonner au contenu des menaces et de faciliter l'intégration avec des technologies tierces, pour inclure les magasins d'applications, les marchés et les intégrations

- Recherche fédérée dans divers environnements
- Fonctionnalité de recherche décentralisée pour interroger les événements en dehors du référentiel de données SIEM et extraire des informations supplémentaires enrichissantes le cas échéant
- Technologies complémentaires, souvent sous la forme de détection et réponse des points finaux (EDR), de détection et réponse réseau (NDR)
- Intégration de la plateforme de lac de données pour le stockage
- Stockage des données essentielles sur les événements de sécurité à long terme et mise à disposition pour la recherche

Quadrant magique

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



Points forts et mises en garde du fournisseur

Dévo

Devo est un visionnaire dans ce Magic Quadrant. La plateforme Devo , une solution SIEM cloud native, séduit les entreprises disposant de grands ensembles de données, ainsi que les organisations de taille moyenne qui disposent d'équipes de centre d'opérations de sécurité (SOC) de maturité moyenne à élevée . Devo propose trois packages : Intelligent SIEM Starter, Intelligent SIEM et Intelligent SIEM+, et la licence est basée sur le volume de données ingérées. La majorité de la clientèle SIEM de Devo est composée d'organisations en Amérique du Nord, tandis que le plus petit nombre est situé en Amérique latine . Au cours de la dernière année, Devo a apporté des améliorations en matière d'analyse avancée du comportement, d'investigation, d'automatisation et d'orchestration. Devo investit dans son AuDRA AI pour le développement de playbooks.

Forces

- **Automatisation du SOC :** en déchargeant le travail manuel des analystes SOC, Devo DeepTrace crée des traces de menaces d'activités suspectes et de chaînes d'attaques via la technologie graphique et le traçage des attaques. Cela automatise les éléments de collecte et d'interprétation des données et réduit l'effort global requis pour créer des rapports d'incident complets.

- **Package simple :** Devo propose trois packages avec des niveaux croissants d'analyse et d'automatisation : Intelligent SIEM Starter ; SIEM intelligent, avec des analyses illimitées du comportement des utilisateurs et des entités (UEBA) et une orchestration, des analyses et des rapports de sécurité (SOAR) ; et Intelligent SIEM+, qui ajoute Devo DeepTrace. Les clients peuvent choisir en fonction de leurs besoins et de leur budget.

- **Évolutivité et accessibilité :** la solution SIEM de Devo facilite l'ingestion de données via un nombre supérieur à la moyenne d' API et de connecteurs prêts à l'emploi (OOTB) .

Précautions

- **Market presence:** Devo continues to invest and expand its customer base; however, its visibility is still limited among SIEM buyers, both "greenfield" and more established.

- **Third-party data lake integrations:** Although Devo's SIEM can integrate with third-party data lakes for querying, the number of integrations is limited compared to some competitors in the market.

- **SAP workloads:** Organizations needing to protect SAP systems will not receive that capability OOTB. Devo depends on a third-party partnership with RHONDOS, which then allows customers to monitor the security and performance of their SAP environment.

Elastic

Elastic is a Visionary in this Magic Quadrant. Its focus is on providing enterprise-grade search and security analytics functions. Elastic's SIEM strategy includes an endpoint security agent for additional host telemetry collection. Elastic uses storage- and compute-based pricing models to charge for Elastic Security. Elastic attracts small, midsize and enterprise clients, primarily in North

America and Europe, and is expanding in the Asia/Pacific (APAC) region. Elastic is investing in its Elastic AI Assistant to accelerate security workflows.

Strengths

- **Query language:** Elastic's query language, ES|QL, lends its strength to many SIEM uses, such as threat intelligence enrichment, incident analysis and threat hunting. Clients can build, save and schedule complex queries, and use the query performance tools to ensure that their queries run as anticipated and don't overconsume resources.
- **Flexible user interface (UI):** Elastic's interface has a wide range of highly extensible features. Clients can customize dashboards and visualization by using a number of built-in options, or use the editor for extended flexibility. This strength will help clients seeking to create custom visualization and monitoring environments for specialized applications.
- **API and number of integrations:** Elastic has made strong investments in an API strategy and has an above-average number of OOTB integrations. Clients can choose to pull data into Elastic via APIs for a wide range of cloud and application sources.

Cautions

- **Advanced UEBA features:** Elastic has OOTB UEBA functionality for common use cases. Advanced users will not find the same levels of customization available in UEBA as in other areas such as dashboarding and data processing.
- **OOTB compliance reports:** Although Elastic's query functions can give a good view into data analysis, standardized reporting functions such as compliance objectives for PCI/DSS and GDPR are lacking compared to others in this research.
- **External endpoint detection and response (EDR) integrations:** Elastic has no out-of-the-box bidirectional integrations with third-party EDR providers outside of its own EDR product. Some clients with existing investments in endpoint security technology may find Elastic's inclusion of its agent a drawback to the overall detection strategy.

Exabeam

Exabeam is a Leader in this Magic Quadrant. Exabeam's solution is Exabeam Fusion SIEM. These products are deployable in hybrid cloud or available as SaaS. Cloud Archive (extra long-term search and storage) and Incident Responder (extended SOAR capabilities) are add-ons at an extra cost. Licensing is term-based and based on the data volumes ingested. The majority of Exabeam customers are in North America and Europe, with a growing presence in the APAC region. Most customers are large enterprises. Exabeam is expanding its centralized management and monitoring of the data pipeline to support enhanced parsing, event building, enriching and data filtering, as well as troubleshooting for better service health monitoring, clear error messaging and alerting.

Strengths

- **User interface:** The Exabeam user interface capabilities strongly align with the needs of security analysts. An example is the strong out-of-the-box dashboards.

- **Live access to third-party data:** Exabeam SIEM can display and process live data from third-party systems such as data lakes, enabling the platform to operate in a more decentralized fashion.

- **Risk-scoring features:** Exabeam's SIEM dynamic scoring capabilities enable clients to take a user-driven view of security issues, linking discoveries together to get more effective scoring in real time, aiding alert suppression and prioritization.

Cautions

- **Onboarding time:** The Exabeam SIEM platform requires a higher-than-average amount of professional service days to configure environments — most of which are enterprise-sized — than other vendors' solutions evaluated as part of this research.

- **Enterprise customer focus:** Exabeam predominantly focuses on the needs of enterprise customers. Smaller organizations should satisfy themselves that the approach and use-case focus is appropriate for their needs before purchasing.

- **Above-average cost:** The Exabeam SIEM platform's above-average selling price should be noted by potential customers for whom price is the deciding factor.

Fortinet

Fortinet is a Challenger in this Magic Quadrant. Its SIEM solution is FortiSIEM. FortiSIEM includes Advanced Agents (for Windows-based UEBA). Add-on solutions include FortiSOAR and FortiAnalyzer, along with the rest of Fortinet's security product suite. FortiSIEM is available as a virtual or physical appliance or as SaaS. On-premises deployment pricing is based on concurrent users for SOAR, devices' events per second (EPS) and the number of agents for SIEM. FortiSIEM Cloud pricing is based on both compute and storage. Licensing is based on devices, and perpetual or subscription licenses are available. It has a global footprint and customers in all major world regions, but especially North America and Europe. Fortinet has invested in GenAI and will offer FortiAI that uses FortiSIEM and FortiSOAR SecOps products to help optimize threat investigation and response, SIEM queries, SOAR playbook creation, and more.

Strengths

- **Integration with broader Fortinet Security Fabric:** Fortinet is a good choice for those widely invested in other Fortinet products. Fortinet Security Fabric enables the formation of a comprehensive security solution by integrating Fortinet products.

- **Built-in configuration management database (CMDB):** Fortinet's centralized CMDB helps with IT infrastructure information discovery of devices, users and applications of organizations. Content filtering is also available.

- **Globally literate:** Fortinet's global customer support coverage places sales teams and local support associates in every major geography. Its SIEM product set is also delivered in a larger

number of native languages than its competitors.

Cautions

- **External data lake integrations:** Fortinet supports Elastic or Open Search as external data lake technologies.
- **Cloud platform adoption:** Fewer customers have deployed Fortinet's SaaS platform, choosing the on-premises version, compared with other vendors in this research. FortiSIEM Cloud has near feature parity to the on-premises edition.
- **Coverage for monitoring cloud environments:** FortiSIEM's cloud security coverage is not as strong as that of other competitors. The only cloud access security brokers (CASBs) supported are Fortinet's own FortiCASB product and Oracle CASB.

Google

Google is a Visionary in this Magic Quadrant. Google's Chronicle SaaS solution has been the foundational product for Google's cloud security strategy, with a focus on large-scale query capabilities. Google's product enhancements for more classic SIEM functions have opened up Chronicle as a viable SIEM competitor. Per-user licensing is available, as well as licensing based on a GB-per-day ingest rate for those with a high user or employee population. Google has a global footprint and customers in all major world regions, but primarily in North America and Europe. Google has made a number of notable acquisitions: Siemplify's SOAR and incident handling as well as Mandiant's detection content and threat intelligence have enhanced the Chronicle SaaS. Google is investing in its Gemini AI for content generation, search, and investigation and threat intelligence summarization.

Strengths

- **Easy-to-use query interface:** Chronicle query is good for both simple and advanced queries. It shows real-time data relationships, which is helpful for threat hunting or rapid investigations. Google is leveraging its well-known fast search capabilities to deliver rapid log analytics and query.
- **Capabilities:** Chronicle's integrated SOAR allows for collaborative incident management functions under its Enterprise+ license. Chronicle also has native threat intelligence capabilities provided by Mandiant.
- **Flexible cost model:** Chronicle allows per-user pricing with unlimited ingestion for the entire organization model, or an ingestion model.

Cautions

- **SaaS-based solution:** Chronicle is only available as a SaaS in Google Cloud Platform (GCP). Cloud self-hosted or on-premises options are unavailable.
- **Reporting:** Chronicle has embedded reporting capabilities through its Looker reporting tool, but has no OOTB compliance content.

- **UEBA features:** Chronicle's UEBA capabilities may be challenging to less advanced users who rely on OOTB content.

Gurucul

Gurucul is a Visionary in this Magic Quadrant. Its analytics-driven next-gen SIEM offers UEBA, identity analytics, fraud analytics, network analysis and SOAR. Gurucul offers flexible pricing options including all-inclusive per-asset/user pricing, ELAs, module-based, data volume/EPS-based pricing, and platform-based pricing. The extensive use of analytics for building risk-based behavioral detections should appeal to enterprise clients requiring complex or fraud-based detections. Gurucul's customer base is composed primarily of large enterprises based in North America, EMEA, APAC. Gurucul is expanding its detection and response capabilities to monitor AI and large language model (LLM) tools.

Strengths

- **Behavioral detection capabilities:** With extensive built-in intelligence and tuning capabilities, Gurucul's SIEM allows clients to build out custom advanced detections involving users, data and other objects.
- **Flexible and extensible architecture:** Gurucul's multicloud architecture lets clients mix and match cloud data sources and back-end storage options, which may save the cost of data transport or duplication.
- **Risk profiling:** Gurucul's risk profiling system automatically creates groups of like objects and scores them against baseline for simplified threat identification and automatic incident prioritization.

Cautions

- **Built for advanced users:** Gurucul's SIEM is more suited to larger and mature security buyers with complex use cases, who have time and experience.
- **SOAR integration:** The SOAR capability on Gurucul lacks some of the advanced features of others, but is included as part of the core component.
- **Marketing execution:** Gurucul has made strides in marketing, but the company and its solutions are still less visible in the SIEM market.

Huawei

Huawei is a Niche Player in this Magic Quadrant. Its SIEM solution is called HiSec Insight and includes Huawei Cloud Security Brain, with numerous additional modules and companion technologies for feature- or architecture-specific requirements. Deployment options include Huawei public cloud for SaaS, customer private clouds and on-premises. Pricing for on-premises deployments is based on data velocity (EPS) and volume (GB per day), with additional charges for log retention and add-on modules. SaaS deployments are based on a GB-per-day ingest rate. Its SIEM customers are largely concentrated in China, although a smaller number of clients are based

in the Middle East, Africa and Latin America. Huawei SecMaster has been created to provide a service that uses the Huawei Security toolset to provide managed detection and response (MDR).

Strengths

- **Expanded threat detection:** HiSec Insight has a threat detection engine based on deep neural network algorithms and ML technology. Predefined playbooks and integrations are offered for automated threat handling.
- **Multisource data collection:** Huawei has an extensive integrated product ecosystem to enable threat handling, as well as a number of APAC-region-specific integrations.
- **Advanced visualization capabilities:** Huawei's threat knowledge graph-based inference analysis and visualized policy orchestration enable easy operation and management. Its Attack Path Visualization displays the entire attack transmission chain.

Cautions

- **Common SaaS monitoring:** Huawei does not offer integrations with Microsoft 365, Google Workspace, or applications from Workday, Salesforce or Box. Cloud infrastructure monitoring is not available outside of Huawei's own cloud.
- **Geographical presence:** Huawei's customer base exists largely in China and the APAC region. Its presence is limited in EMEA and Latin America, and there is no customer presence or deployment infrastructure in North America.
- **Data lake integrations:** Huawei supports only its own data lake technology, limiting clients' ability to expand and enrich detections and coverage.

IBM

IBM is a Leader in this Magic Quadrant. IBM Security QRadar SIEM can be deployed via on-premises software, in a public or private cloud, or via SaaS as QRadar on Cloud (QROC). IBM also offers QRadar SOAR, Vulnerability Manager, EDR and Attack Surface Management as other products in the QRadar suite. Licensing for QRadar SIEM is based on EPS and/or flows per minute (FPM). IBM has introduced single-metric pricing based on Resource Units (RUs) for the QRadar suite. IBM's customer base is composed primarily of midsize and large enterprises based in North America, EMEA, APAC and Latin America. IBM is investing in incorporating generative AI into their Unified Analyst Experience.

Strengths

- **Extensive security business and presence:** IBM has the global reach required to deliver its products, support and services in every major geographic region.
- **Integration across IBM security:** IBM offers a wide range of optional, tightly integrated add-on solutions and service offerings to complement and support QRadar SIEM. Additional capabilities include network security, vulnerability assessment, ASM, customized threat

intelligence reports, data protection, its compliance automation reporting tool (CART) and MDR services.

- **Native exposure context data:** QRadar has native capabilities to enrich assets with exposure data, allowing users to easily react preventatively to threat detections. Add-on capabilities expand this to include continuous automated testing through Randori Recon.

Cautions

- **Pricing complexity:** Although IBM has made some adjustments on its licensing and pricing schemes, QRadar still has several different pricing options that may present a complex set of choices for potential and current customers.

- **Sales and customer support:** Due to IBM's size and the number of products it offers, customers may experience challenges engaging and obtaining timely responses on bids. Organizations should confirm with the sales team how the relationship and process will support their requirements.

- **Prebuilt SOAR integrations and playbooks:** Organizations that lack SOAR expertise will want to confirm that needed integrations and playbooks are available OOTB and plan accordingly.

Logpoint

Logpoint is a Niche Player in this Magic Quadrant. Its simple pricing model is based on a base level of the ingestion of each employee and the number of employees. Logpoint Converged SIEM includes SOAR functionality. SOAR is included with a single-seat license included with the base level. Logpoint offers UEBA and Business-Critical Security (BCS), which adds support for SAP, and both are available separately at additional cost. Deployment options include SaaS, customer private clouds and on-premises. A Europe-based company, Logpoint has its greatest number of customers in its home region and has a small footprint internationally. Summa Equity acquired Logpoint in 2023.

Strengths

- **Simple licensing models:** Logpoint's employee-based model allows for simplification of many of the planning and sizing variables, making their SIEM pricing predictable. A one-seat SOAR license is included.

- **Dashboard customization:** Logpoint allows clients to set up a variety of roles and usages for the product. Organizations will find Logpoint's extensible UI supports custom monitoring.

- **Scalability and accessibility:** Logpoint's SIEM solution provides ease of storage for security data with an above-average number of native analytics available OOTB that support the speed and ease of detection.

Cautions

- Geographical presence: Logpoint's customer base and sales exist largely in Europe. Its presence is limited in North America and APAC. Customers should ensure that the sales and

support options will meet their needs in their local area; this includes local compliance requirements.

- UEBA abilities: Logpoint does not include the ability to create customized UEBA models. Advanced users will not be able to create extended new user and entity behavior analytics for themselves.

- Threat intelligence: Logpoint's lack of an internal threat intelligence feed requires the use of a third-party or open-source threat intelligence platform (TIP) for integration in detection content. Threat enrichment SOAR playbooks are a roadmap item.

LogRhythm

LogRhythm is a Niche Player in this Magic Quadrant. LogRhythm has three platforms: LogRhythm SIEM includes several add-on components to deliver endpoint, network and UEBA capabilities; LogRhythm Cloud is a cloud-hosted version of SIEM; and LogRhythm Axon is a cloud-native SIEM platform. Licensing is available on a perpetual or subscription basis (messages per second per day) or an unlimited basis (priced by the number of identities) for the self-hosted option. LogRhythm Cloud is licensed by messages per second and terabytes of online storage. LogRhythm Axon is licensed by daily ingest rate and days of searchable data. The majority of its customers are in North America and Europe. Customers are both large enterprises and midsize customers. LogRhythm invests in deeper integration with LogRhythm NDR to both SIEM and LogRhythm Axon platforms.

Strengths

- **Compliance reporting:** LogRhythm's platforms have a higher-than-average number of supported compliance standards and reports for those clients needing to implement compliance and security reporting.

- **On-premises solution:** LogRhythm's roadmaps show that it has a long-term commitment to improving the on-premises SIEM alongside LogRhythm Axon development.

- **Global coverage:** LogRhythm has invested in a global sales force in every major geography, so the number of days needed to bring its solution online is well below the average among vendors in this research.

Cautions

- **LogRhythm Axon solution:** LogRhythm Axon is a separate product line from LogRhythm SIEM and Cloud SIEM, and their respective capabilities differ. Potential buyers should compare capabilities and roadmap when evaluating LogRhythm's products.

- **Cloud strategy:** LogRhythm maintains two cloud-hosted product lines. With LogRhythm Axon being the newer, cloud-native solution, current and prospective users of LogRhythm Cloud should validate LogRhythm's long-term commitment to this offering.

- **Capabilities:** LogRhythm SIEM does not support a chat facility, or importing rules using Sigma or Yara, which may be important to some users.

Logz.io

Logz.io is a Niche Player in this Magic Quadrant. Logz.io Cloud SIEM is available as a cloud-based deployment. Threat intelligence is an included add-on with every install. Logz.io Cloud SIEM is licensed by log data ingested per day as well as data retention period. Most of its customers are in North America and Europe, and it has diverse client sizes. Logz.io is investing in expanding its unsupervised machine

learning tools to increase the system's ability to automatically detect and respond to events.

Note: Logz.io advised Gartner in February 2024 that it is now focused completely on delivery of full stack observability with its Open 360 platform and does not consider itself a stand-alone SIEM vendor.

Strengths

- **Intelligent storage:** Logz.io allows data to be moved between multiple storage tiers to optimize resources and minimize related costs. Amazon S3 is utilized for cold storage to further enable cost management.
- **Language support:** Logz.io supports the highest number of languages among vendors in this research, enabling global SOCs to work in their native language.
- **Observability tooling:** The Logz.io platform can integrate metrics and tracing telemetry. Combined sources of data simplify the data collection and costs into one provider.

Cautions

- **Out-of-the-box detection and compliance:** The number of correlations, analytics and reports available OOTB for standard use cases, compliance requirements and standards is lower than the average among vendors in this Magic Quadrant.
- **SOAR capabilities:** Lack of any inbuilt SOAR features requires acquisition of a supported third-party SOAR, which will increase costs and complexity for architecture, integration and workflow for incidents.
- **Advanced analytics capabilities:** Logz.io lacks advanced capabilities such as advanced analytics, supervised ML and deep learning analytics. These are required to build out extended detection and correlate extremely large sets of data and logs.

ManageEngine

ManageEngine, a division of Zoho Corp., is a Niche Player in this Magic Quadrant. Its SIEM solution, Log360, is cloud-based and deployed from its data center. UEBA, SOAR and data loss prevention (DLP) are included add-ons in the SaaS license. In addition, ManageEngine offers security products such as Firewall Analyzer, Vulnerability Manager Plus and FileAnalysis. Licensing is based on the amount of data stored per day in the cloud over a specific period. Its customers are primarily large and midsize enterprises who are located in North America, Europe

and APAC. ManageEngine is investing in its Vigil IQ engine to enhance advanced threat detection use-case support and expanded vendor integrations.

Strengths

- Expanded reporting engine: ManageEngine's reporting engine is comprehensive, supporting numerous compliance-framework-focused outputs and alerting based on compliance violations.
- Global presence: ManageEngine has the global reach required to deliver its products, sales, support and services in every geographic region.
- Native SOAR capabilities: ManageEngine for response and workflow automation is included with the base license.

Cautions

- **Advanced SOAR capabilities:** ManageEngine's native SOAR does not support features such as playbook testing and playbook sharing.
- **Compatibility with third-party data lakes:** ManageEngine's product does not support recalling data from third-party external data sources, including external data lakes.
- **Community app store:** ManageEngine lacks an app store where its customers can share workflows, custom detections and parsers.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its SIEM solution is Microsoft Sentinel, which is delivered only as a SaaS offering via Microsoft's Azure cloud services. Pricing is based on volume of data analyzed in Microsoft Sentinel and is variable based on level of subscriptions in Microsoft 365 E5, A5, F5 and G products that include daily allowances. Charges are also levied for data stored in Azure Monitor Log Analytics workspace by retention period and volume. Committed tiers and pay-as-you-go models are available. Microsoft Sentinel's customer base spans North America, EMEA, APAC and Latin America, and organizations of all sizes from small and midsize businesses (SMBs) to large enterprises. Microsoft's Security Copilot has plans for incident response, and integration with other Microsoft tools.

Strengths

- **Highly integrated ecosystem:** Microsoft Sentinel has native integration with broader Microsoft security offerings: CASB, identity, endpoint, network, operational technology (OT) security, and UEBA and SOAR tools. The onboarding process for supported data sources is simplified with the help of codeless connectors and data normalization capabilities built directly into the Microsoft platform.
- **Customizable solution:** Microsoft Sentinel customers can build and customize ML-based threat detection models by leveraging native integration with Azure Synapse (a paid add-on), along

with OOTB templates. The Microsoft Sentinel threat intelligence dashboard provides a fully customizable canvas for reporting on the health and performance of TI.

- **MITRE ATT&CK coverage:** Microsoft Sentinel offers strong MITRE ATT&CK coverage built around the entire Microsoft security toolset. Strong coverage enables analysts to understand what the next steps of an attack may be.

Cautions

- **Reliance on Azure capabilities:** Sentinel runs within the Azure ecosystem and relies on other Azure services for various functionalities. The learning curve can be steep without familiarity with Azure workflows and UIs.
- **OOTB compliance reporting:** Microsoft Sentinel has comparatively limited OOTB compliance reporting.
- **Deployment:** Sentinel is available only as a SaaS product hosted in Microsoft Azure. Cloud self-hosted or on-premises options are unavailable.

NetWitness

NetWitness is a Niche Player in this Magic Quadrant. NetWitness SIEM is part of a larger platform that can be connected to several add-on components to deliver endpoint, network and user behavior analytics capabilities. SaaS licensing is available on a GB-per-day ingest rate plus length of retention, and a per-user cost for UEBA. NetWitness's SIEM customers are primarily large enterprises based in North America, Europe, APAC, the Middle East and Latin America. Investments in the NetWitness platform will expand the security coverage and provide simplified detection and response solutions.

Strengths

- **Vendor portfolio:** NetWitness is a multicapability platform that will appeal to SOCs that want a single vendor for modern SOC instrumentation, including integrated SIEM, UEBA, SOAR, EDR and network threat analytics.
- **Global presence:** NetWitness has the global reach required (via direct and partner channels) to deliver its products, support and services in every geographic region.
- **Simple deployments:** NetWitness's number of days needed to bring its SIEM solution online is lower than average among vendors in this research, showing that the system can easily be taken from install to usable in a short time.

Cautions

- **SaaS adoption:** Fewer customers have deployed NetWitness's SaaS platform, compared with other vendors included in this research. Most customers opt for its on-premises version.
- **UEBA customization:** When compared to other vendors in this Magic Quadrant, NetWitness has a limited number of customizations in UEBA, making it harder for customers to build custom use cases.

- **Out-of-the-box reporting features:** Reporting for standard compliance requirements and standards is lower than average when compared to other vendors in this research.

Odyssey

Odyssey is a Niche Player in the Magic Quadrant. Its SIEM solution is a component of its broader ClearSkies Threat and Vulnerability Management Platform. It is based on Apache Hadoop, and hosted in Microsoft Azure for the Americas and two private clouds for other regions. Add-on modules include EDR, Active Defense, Identity & Access, and DNS Shield — usually at an additional cost. Odyssey's licensing is consumption-based and priced in GBs per day. The majority of Odyssey's SIEM customer base is located in the EMEA region and appeals to a mix of small, midsize and large organizations. Odyssey is investing in natural language processing (NLP) and LLM integrations.

Strengths

- **Third-party app marketplace:** In 2022, Odyssey released a marketplace to provide an improved user experience for integrating detection content and other third-party security controls into its SIEM solution.
- **Extensive product ecosystem:** Odyssey offers a number of integrated capabilities, including EDR, vulnerability assessment, UEBA, security orchestration, automation and response, and identity and access management.
- **Quantity of correlation rules:** Odyssey offers a large number of correlation rules OOTB when compared to other SIEM vendors in this research. Organizations with a diverse and complex environment should factor this into their assessment.

Cautions

- **Third-party SOAR integration:** Odyssey's SIEM solution does not support bidirectional integration with third-party SOAR platforms; therefore, organizations with already-deployed SOAR technology must ensure Odyssey's native SOAR capability meets workflow automation requirements.
- **Europe-centric availability:** The majority of Odyssey's salesforce is based in the EMEA region, with a very small percentage in North America and APAC. For clients with global requirements, lack of understanding of local market requirements and restrictions can lead to poor experience from a sales and support perspective.
- **Advanced customization and some common modern SIEM features:** Odyssey has lower-than-average abilities in data science model/algorithm creation and API integration development features compared with its peers in this research. It may not support mature organizations with a dynamic set of threat detection, data manipulation and reporting requirements. In addition, it does not support federated searching.

OpenText

OpenText (previously Micro Focus) is a Visionary in this Magic Quadrant. Its SIEM solution, ArcSight, includes SIEM, UEBA, SOAR and TIP functionality. There is a cloud-hosted deployment option. Licensing is available on a perpetual or subscription basis (events per second per day) and managed entity (priced by the number of identities) for ArcSight Intelligence (UEBA) or OpenText EnCase (EDR). OpenText's operations, other than Latin America, are geographically diversified, and its client profile is predominantly midsize and large enterprises. OpenText's acquisition of ArcSight allows it to expand the security platform.

Strengths

- **Threat intelligence platform capabilities:** A basic TIP solution is included with ArcSight SIEM. It provides MISP open-source intelligence to all ArcSight buyers at no additional cost. Customers can upgrade to advanced threat intelligence, which provides premium threat intelligence feeds.
- **SOAR included with SIEM:** ArcSight ESM includes SOAR capability at no additional charge for this feature. Users can leverage a graphical canvas to create workflows or leverage a code-based development interface for more complex playbook creation.
- **MITRE ATT&CK mapping:** OpenText's platform offers a more extensive mapping of detection content to the MITRE ATT&CK framework. This supports understanding attack coverage, and provides guidance on available coverage content.

Cautions

- **UEBA model creation learning curve:** Predictive Model Markup Language (PMML) is used to create models, which can take time to master for those that have not used it before or are not from a data science background.
- **Compatibility with third-party data storage:** ArcSight does not support searching data from third-party storage, although it does support dashboarding and reporting.
- **Implementation time:** On average, OpenText has a greater number of professional service days used to implement the solution than most other vendors in this research. This indicates a high level of complexity to get the solution running.

QAX

QAX is a Niche Player in this Magic Quadrant. QAX SIEM solution NGSOC can be deployed either on-premises or via SaaS. Other capabilities, such as UEBA and SOAR, are offered as add-on modules for an additional cost. Licensing is based on EPS and the number of data sources. QAX's customer base is primarily located in the APAC region, but it also has a presence in MEA. Most clients are midsize, with a few small and large enterprises. QAX is investing in AI Security Assistant to support automatic analysis and investigation in its platform.

Strengths

- **Cost-effective:** QAX has a simple and flexible pricing model, and its average selling price was lower than most other vendors in this Magic Quadrant.

- **Managed detection and response service:** MDR is available directly from QAX at an additional cost. This provides a single source for customers who want access to the SIEM product and need service support for detection and response for all of the QAX solutions.

- **User interface:** QAX's interface can customize dashboards and visualization by using built-in options or an editor for extended flexibility.

Cautions

- **APAC-centric:** QAX predominantly serves customers in one region: APAC. From a sales and support perspective, lack of understanding of local market requirements and restrictions outside of APAC can lead to poor experience for customers with a global footprint.

- **Data lake integrations:** QAX supports region-specific commercial data lake technologies only.

- **SaaS adoption:** Compared to its peers in this research, fewer customers than average have deployed its SaaS platform, choosing the on-premises version instead. This may be due to local regional requirements.

Rapid7

Rapid7 is a Challenger in this Magic Quadrant. Its SIEM solution, InsightIDR, runs on the cloud-native Insight platform. Licensing is on a term license, with a pricing model based on the number of assets monitored. Customers of the InsightIDR SIEM range from small to large organizations concentrated most heavily in the U.S., followed by Europe and APAC. Rapid7's investment in a SOC Analyst Investigative Toolkit brings the SIEM building blocks and digital forensics and incident response (DFIR) capabilities into investigative workflows in a single tool.

Strengths

- **Managed detection and response service:** MDR is available directly from Rapid7 at an additional cost. It represents a single source for customers who want access to the SIEM product and need service support for detection and response.

- **Small and midsize business**: With a higher than average number of SMB clients compared to other vendors evaluated in this research, Rapid7 has a model that supports SMB security needs to get SIEM programs working.

- **Wide range of integrated capabilities:** Rapid7 offers a core SIEM with many security capabilities, including InsightVM, which provides vulnerability management; and InsightIDR, which has EDR, UEBA and network detection and response (NDR) capabilities that are highly integrated for a single experience for SOC operators.

Cautions

- **Compatibility with third-party data storage:** Rapid7's SIEM product does not support recalling data from third-party storage. This may lead to added costs and increased regulatory needs.

- **Advanced customization capabilities:** InsightIDR lacks more advanced capabilities, such as advanced analytics (e.g., supervised ML and custom deep-learning analytics).

- **SaaS only:** InsightIDR is only available as a SaaS solution.

Securonix

Securonix is a Leader in this Magic Quadrant. Its SIEM solution, Unified Defense SIEM, includes an embedded Snowflake data lake, UEBA, basic SOAR and use-case-specific content (such as with specific industries and/or systems). Add-ons include advanced SOAR capabilities, Autonomous Threat Sweeper and Investigate. Licensing is based on EPS and is typically offered via a subscription. Perpetual licensing is available only by exception. Most Securonix customers are in North America, followed by EMEA, APAC and Latin America. Securonix's customer base is made up primarily of large enterprises and midsize organizations. Securonix is investing in its AI Genie to improve SOC efficiency by improving ingestion automation, search simplicity and threat detection logic.

Strengths

- **Third-party data lake access:** Unified Defense SIEM is able to query and display live data from third-party systems such as data lakes (e.g., Snowflake and Databricks), enabling the platform to operate in a more decentralized fashion.
- **Leveraging digital risk protection data:** Securonix partners with threat intelligence and digital risk protection service vendors to embed darknet and social media monitoring intelligence to feed into its TIP and Autonomous Threat Sweeper for enhanced alert enrichment and prioritization of threats.
- **Health and use-case effectiveness of SIEM:** Securonix provides users insights via a dashboard into operational metrics, KPIs and benchmarks to help improve the effectiveness of the SIEM's configuration and threat detection content (such as identifying missing data sources, correlation rules and analytics modules for critical use cases).

Cautions

- **FedRAMP certification:** Although Snowflake, the back end of Securonix's log management capability, is FedRAMP-certified, Securonix is not.
- **License model:** Securonix uses a consumption-based model that considers EPS instead of the now common ingest-based model. Users should validate the licensing model as part of their evaluation.
- **Deployment:** Professional services are not required, but Securonix has a higher than average number of professional services days for deployment into cloud environments.

Splunk

Splunk is a Leader in this Magic Quadrant. Splunk's Enterprise Security application is delivered either on-premises or via SaaS. Splunk offers pricing flexibility based on either daily ingest, or on cloud workloads, known as Splunk Virtual Compute. The majority of Splunk's clients are larger North America-based enterprise organizations. Splunk is introducing an AI Assistant for Security

integrated with Enterprise Security to provide detection and response capabilities. Cisco completed its acquisition of Splunk on 18 March 2024.

Strengths

- **Overall observability:** The Splunk platform can integrate security, IT, application and other data sources. This, coupled with its federated search and analytics capabilities across third-party data stores, is a strength for clients seeking to build highly enriched queries and alerts.
- **Extensive integration:** Splunk's integration of SOAR enhances a wide range of common SIEM use cases. Clients wanting quick time to production automation for common SIEM operational functions will find Splunk's library of playbooks a strength.
- **User interface:** Splunk's UI and dashboard provide significant customization. Clients requiring custom animations and visualization for specialized monitoring, such as OT or financial systems, will find the UI editor an overall strength.

Cautions

- **Pricing:** Splunk has a higher-than-average cost compared to other vendors evaluated in this research. With increasing demands to log everything, prospective clients should evaluate the costs versus security value of the data.
- **Complexity and expertise:** With a higher-than-average number of days of professional services needed to implement Splunk, clients need to ensure that they have the needed staffing or outsourced providers to see value from the tool.
- **Regional sales support:** The majority of Splunk's salesforce is based in North America. Sales support may be limited or delivered via value-added resellers outside of North America.

Sumo Logic

Sumo Logic is a Challenger in this Magic Quadrant. Its SIEM product, Sumo Logic Cloud SIEM Enterprise, is delivered as a SaaS-only solution as part of its SaaS log analytics platform. Licensing Cloud SIEM Enterprise 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. Sumo Logic's customer base is a mix of small, midsize and enterprise customers, with the majority based in North America; however, it has a growing presence in Europe, Latin America and Asia/Pacific. In May 2023, Sumo Logic was acquired by Francisco Partners.

Strengths

- **MITRE ATT&CK support:** Users are able to track coverage based on out-of-the-box rules that enable users to understand coverage.
- **Model-building assistance:** Sumo Logic has a feature called Insight Trainer that builds models via investigated insights to suggest tuning recommendations and severity adjustments on rules.

- **FedRAMP certification:** Sumo Logic Cloud SIEM Enterprise is one of the few SIEM solutions in the market that is FedRAMP-certified as a Moderate Impact system.

Cautions

- **Regional sales support:** The majority of Sumo Logic's sales force is based in North America. Potential buyers should ensure the sales force understands regional requirements.
- **Searching across distributed data stores:** Organizations requiring search capabilities across logs and other data distributed across multiple external and non-native data stores may need to confirm these are available from Sumo Logic.
- **OOTB compliance reports:** Sumo Logic does not have the breadth of compliance reports and dashboards OOTB when compared to other vendors in this research.

Venustech

Venustech is a Niche Player in this Magic Quadrant. Venustech's SIEM solution is Unified Security Management (USM). Most clients have deployed the on-premises version, but a cloud-hosted deployment option exists. Other products include Unified Threat Management (UTM), Venusense Traffic Anomaly Detection and Mitigation System (Venusense ADM), Venusense Network Traffic Analysis (NTA) and Venusense Web Application Firewall (WAF). USM is licensed by one of three feature sets and the number of management nodes: Basic package includes standard SIEM tooling; Package A adds Playbooks and China MLPS compliance support; and Package B adds UEBA and ML support. Most of Venustech's customers are in Asia/Pacific. Venustech is investing in its intelligent security operation LLM for chat-based interactions for security issues.

Strengths

- **Advanced analytics capabilities:** Venustech's advanced capabilities, supervised ML and UEBA are able to support a more advanced security team.
- **Threat detection, investigation and response capability:** Venustech offers a core SIEM with a multitude of security capabilities including EDR and NDR. All of these capabilities offer a single experience for SOC operators.
- **Simple SaaS license model:** Licensing based on base price standard, premium, enterprise, or number of managed hosts ensures that security teams do not have any unexpected costs.

Cautions

- **UI translation:** Some advanced features have not been translated into English. Prospective clients should require an estimated release date on necessary features.
- **APAC-centric:** Venustech predominantly serves customers in one region: APAC. From a sales and support perspective, lack of understanding of local market requirements and restrictions can lead to poor experience for prospective clients with presence outside of this region.
- **Large enterprise focus:** The majority of Venustech clients are midsize and large enterprises.

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.

Added

The following vendors met the commercial and functional requirements for inclusion in the 2024 Magic Quadrant:

- Google
- Logz.io
- NetWitness
- Odyssey
- QAX
- Venustech

Dropped

No vendor from the 2022 Magic Quadrant for SIEM was dropped for 2024.

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts consider 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 consumable by end-user customers as cloud-native [1] software and/or SaaS, excluding those that are available only as part of a managed security services relationship. SIM and SEM must-have capabilities are:
  - Collect infrastructure details and security relevant data from a wide range of assets located on-premises and/or in cloud infrastructure.
  - Ability for end users to self-develop, modify and maintain threat detection use cases utilizing correlation, analytic and signature-based methods.
  - Correlate and apply both SIEM vendor- and client-created analytics to collect, normalize and contextualize event data from disparate sources, using multiple mechanisms (log stream, API, file processing), for the purposes of threat detection, use-case implementation and incident investigation.

    - Provide case management and support incident response activities. [2]
    - Generate reports to support business, compliance and audit needs.
    - Store essential security event data over the long term and make it available for investigation.
- At least 50 vendor-provided collectors for data capture and streaming from heterogeneous third-party data sources via API in addition to data streaming or log collection. This must include formally recognized partnerships with at least 10 major technology vendors.
- A product that supports behavioral analysis and/or correlation of data from sources other than directly from the vendor's product ecosystem, this should include market-leading network technologies, endpoints/servers, cloud (IaaS or SaaS), and business applications.
- Features, functionality and 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 as of 31 March 2023:
    - Federated search into distributed environments, able to search across SIEM data repositories (e.g., geographic regions or cloud provider's regions)
    - Search functionality to query events outside the SIEM data repository and to pull in additional enriching information where appropriate
    - Third-party data lake platform integration storage
    - Availability of long-term data storage and reporting (with "hot" recall capability of 365 days)
- 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 31 March 2023:
    - Security orchestration automation and response (SOAR)
    - Threat intelligence platform (TIP)
    - Advanced analytic capabilities using user entity behavior analytics (UEBA), data sciences (e.g., supervised and unsupervised machine learning, deep learning/recurrent neural networks)
- Cloud-native/SaaS license and maintenance (excluding managed services) revenue exceeding $75 million for the 12 months prior to 31 March 2023, or have 200 distinct production [3] customers with direct contracts on cloud-native or SaaS platforms as of the end of that same period.
- In the 12 months prior to 31 March 2023; to have received 15% of SIEM cloud-native/SaaS revenue from buyers with headquarters outside the geographic region [4] of the vendor's

headquarters location, or having at least 30 production customers, each with headquarters outside the geographic region of the vendor's headquarters location.

- Evidence of online marketing campaigns, events or promotions from third-party media sources targeting countries in at least two geographic regions, distributed prior to 31 March 2023.
- Cloud-native/SaaS SIEM platform hosted in more than three major geographic regions.

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. [5]

Honorable Mentions

- **Anvilogic** did not meet the commercial requirements for inclusion in this Magic Quadrant. However, it is considered an option for buyers who are focused on having an analytics layer on top of their data lake.
- **CrowdStrike** did not meet functional requirements for inclusion in this Magic Quadrant. Buyers would consider LogScale as an extension of other CrowdStrike technologies.
- **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** was not surveyed as part of this Magic Quadrant process. 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 OOTB under one license.
- **Hunters** did not meet commercial requirements for inclusion in the 2023 Magic Quadrant for SIEM. Hunters provides machine-powered ingestion, detection, triage, and investigation based on a security data lake architecture. It offers unlimited ingestion per entity, which is best for buyers looking to have cost predictability.
- **Logsign** Unified Security Operations (SO) Platform did not meet the commercial requirements for inclusion in this Magic Quadrant. Logsign Unified SO Platform will appeal to buyers familiar with Elasticsearch. It offers a combination of SOAR and SIEM capabilities built around a streamlined user interface with customizable dashboards.
- **Palo Alto Networks** did not meet commercial requirements for inclusion in this Magic Quadrant. Palo Alto Networks' XSIAM is a consideration for buyers looking to integrate into other Palo Alto Networks technologies like the Cortex platform.

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 are 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. Promotion of the brand, increasing awareness of products and influence on the SIEM market are evaluated.

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 and customization of user interfaces.

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

Evaluation Criteria ↓	*Weighting* ↓
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Medium

Source: Gartner (February 2024)

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.

Despite vendors' focus on expanding their capabilities, we continue to value simplicity of deployment and ongoing 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.

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	Low
Offering (Product) Strategy	High
Business Model	NotRated

Evaluation Criteria ↓	*Weighting* ↓
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (February 2024)

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 emphasizes global SaaS architecture availability and multifaceted platform features like SOAR, UEBA, TIP, self-service analytics 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 in the quadrant.

This research assesses vendors based on their solutions as offered through 2022 up to 30 September 2023 to include the strength of their SIEM products and roadmaps. The SIEM market continuously evolves, 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 $5.03 billion in 2022 to $5.7 billion in 2023 (see **Market Share: All Software Markets, Worldwide, 2023**), a 13% annual growth rate compared to a 22% increase 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.

SIEM technologies have become a staple for security operations, with a long-standing position as a technology that has reached the Plateau of Productivity (see **Hype Cycle for Security Operations, 2023**). However, Gartner has seen evidence that the SIEM market itself has been disrupted by external forces that cause clients to rethink the role of a SIEM, and how to select the best technology for them. The forces that have disrupted the SIEM market are:

- The client journey to cloud service providers
- The growing appetite for more security data (cost bloat)
- The need for overall simplicity in their detection stack

As such, SIEM conversations with clients often may include other technologies such as cloud-native security suites, data lake solutions, and XDR offerings.

Data sovereignty and privacy laws will continue to impact data residency and access. SIEM vendors can address this by deploying their solutions regionally and restricting data residency based on buyer requirements. Some are starting to offer clients the ability to use their own data lake solutions as storage, allowing clients to have even more control over their data governance. Data residency is a contributing factor to continued demand for on-premises and cloud self-hosted SIEM.

The disruptive forces within the SIEM market have brought about innovation, with providers marketing themselves to the SIEM buyer from brands that have not traditionally offered a SIEM product. This wave of innovation has challenged the very definition of a SIEM, as well as forced incumbent SIEM vendors to rethink their product roadmap. Generative AI is an emerging capability, but Gartner is yet to see broad implementation by, and feedback from end-user customers. As such, generative AI capabilities and roadmap are not included in the current evaluation.

These movements in the market are limiting all vendors on overall execution. They have also narrowed the overall gap between leading vendors on vision and execution. As a result, the Leaders from the 2022 Magic Quadrant remain; some vendors move between Challengers and Visionaries, based on their trajectory relative to the average execution and vision; and a longer tail of Niche Players emerges.

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

Threat detection:

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

Response:

- SOAR

- TI management
- 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, Active Directory Group Policy settings, etc.)
- Poly-cloud visibility and unified exposure understanding
- Threat detection framework alignment

Compliance:

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

SIEM vendors have already begun investing in (or acquiring) telemetry collection solutions to deliver a prebuilt ecosystem of security technologies for buyers looking for an encapsulated security solution. This aligns with the cybersecurity mesh concept 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, allowing the vendor choice option to persist well into the future.

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 leaders build a compelling business case for purchasing based on outcome-delivered metrics, which can answer questions from the business about what value a SIEM will deliver. (See **Tool: Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security**.)

Evidence

[1] Gartner defines “cloud-native” as something that is designed to leverage cloud characteristics. Those cloud characteristics are part of the original definition of cloud computing. It’s all about capabilities delivered as a service and that are scalable and elastic, metered by use, service-based, ubiquitous by means of internet technologies, and shared.

[2] Incident response activities might include functions such as verbose event recording, chain of custody, automated mitigation actions, and reporting.

[3] Production customers are defined as those that have licensed the SIEM and are monitoring production environments with the SIEM.

[4] Geographic regions are defined as North America, Latin America, Europe, Middle East, Asia, Japan, Africa.

[5] Managed services are defined by Gartner as those in which the customer engages the vendor to establish, monitor, escalate and/or respond to alerts, incidents and cases.

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.

Stratégie marketing : un ensemble de messages clairs et différenciés, communiqués de manière cohérente dans toute l'organisation et externalisés via le site Web, la publicité, les programmes clients et les déclarations de positionnement.

Stratégie de vente : stratégie de vente de produits qui utilise le réseau approprié de filiales de vente directe et indirecte, de marketing, de service et de communication qui étendent la portée et la profondeur de la portée du marché, des compétences, de l'expertise, des technologies, des services et de la clientèle.

Stratégie d'offre (produit) : approche du fournisseur en matière de développement et de livraison de produits qui met l'accent sur la différenciation, les fonctionnalités, la méthodologie et les ensembles de fonctionnalités en fonction des exigences actuelles et futures.

Modèle commercial : la solidité et la logique de la proposition commerciale sous-jacente du fournisseur.

Stratégie verticale/industrielle : stratégie du fournisseur visant à orienter les ressources, les compétences et les offres pour répondre aux besoins spécifiques de segments de marché individuels, y compris les marchés verticaux.

Innovation : Agencements directs, connexes, complémentaires et synergiques de ressources, d'expertise ou de capital à des fins d'investissement, de consolidation, défensives ou préventives.

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