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

Publié le 10 octobre 2022 – ID G00755317 – Durée de lecture : 49 min

Par les analystes : Pete Shoard, Andrew Davies, Mitchell Schneider

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

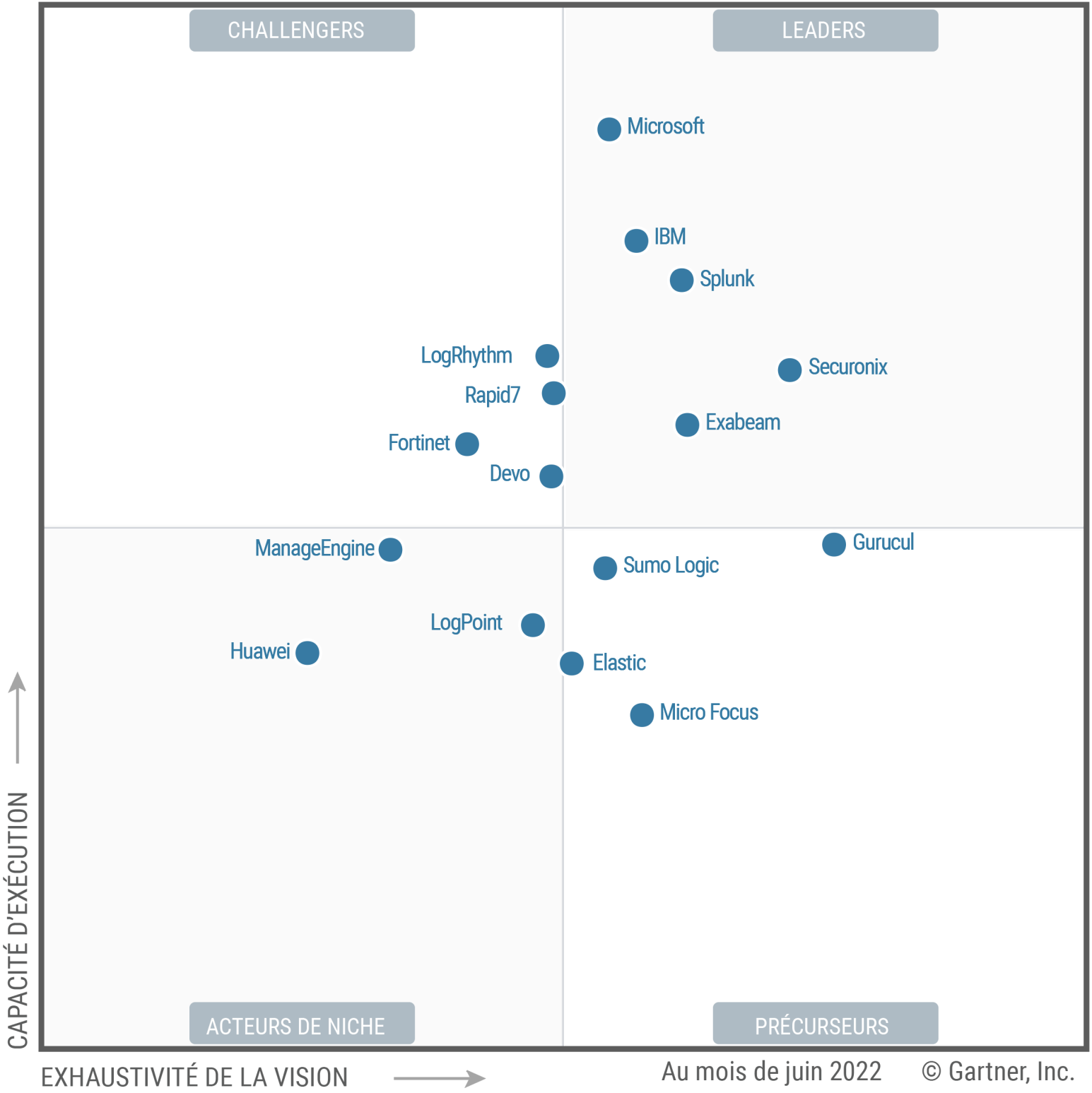
Définition/Description du marché

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

Le SIEM regroupe les données d'événement produites par les solutions de supervision, d'évaluation, de détection et de réponse déployées dans les environnements d'applications, de réseaux, de terminaux et de cloud. Les capacités comprennent la détection des menaces, par le biais de la corrélation et de l'analyse du comportement des utilisateurs et des entités (user and entity behavior analytics, UEBA), et l'intégration des réponses, généralement gérée par l'orchestration, l'automatisation et la réponse en matière de sécurité (security orchestration, automation and response, SOAR). Les rapports de sécurité et le contenu des menaces mis à jour en permanence grâce à la fonctionnalité de la plateforme de threat intelligence (threat intelligence platform, TIP) sont également des intégrations courantes. Bien que le SIEM soit principalement déployé en tant que service basé sur le cloud, il peut prendre en charge le déploiement sur site.

Magic Quadrant

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



Points forts des fournisseurs et réserves

Devo

Devo est un Challenger de ce Magic Quadrant. Son produit SIEM, l'application Security Operations, est livré sous forme d'offre SaaS. La base de clients SIEM de Devo se trouve principalement en Amérique du Nord, suivie par l'Europe et le Moyen-Orient, et est composée de petites, moyennes et grandes entreprises. Début 2022, Devo a obtenu le statut « En cours » pour la norme du Programme fédéral de gestion des risques et des autorisations (Federal Risk and Authorization Management Program, FedRAMP), et prévoit d'obtenir une autorisation complète plus tard dans l'année. Les licences, y compris les fonctionnalités complémentaires (TIP via MISP, stockage à chaud, Entity Analytics et Devo Flow), sont basées sur le volume de données ingérées.

Points forts

- **Observabilité informatique couplée à la sécurité :** Devo offre des capacités d'observabilité et de sécurité informatiques au sein de la même interface utilisateur et fournit des échéanciers solides, ainsi que des vues adjacentes pour une fonctionnalité commune aux équipes de sécurité et d'I&O.

- **Accessibilité des données :** l'outil SIEM de Devo permet aux utilisateurs d'envoyer rapidement et facilement des données dans la solution via son API à tout moment où toutes ces données sont indexées. Par conséquent, les clients peuvent accéder aux données à tout moment, où qu'ils se trouvent et peuvent les exploiter comme ils le souhaitent.

- **Fonctionnalités TIP natives :** Devo fournit la fonctionnalité TIP via MISP sans frais supplémentaires, qui utilise une multitude de flux accessibles au public et envoie les informations à l'outil SIEM pour enrichissement et pour réaliser des détections améliorées.

Réserves

- **Manque de fonctionnalité SOAR native :** la solution SIEM de Devo s'intègre à de nombreux fournisseurs SOAR visibles sur le marché ; cependant, elle n'offre actuellement pas les composants de réponse d'un SOAR.

- **Visibilité limitée sur le marché du SIEM :** bien que Devo ait augmenté ses opérations de vente et étendu ses campagnes marketing, elle n'est pas aussi connue sur le marché du SIEM que certains de ses concurrents.

- **Assistance limitée pour les services de sécurité :** la prise en charge externe de la solution SIEM de Devo par les fournisseurs MSSP/MDR est limitée par rapport aux autres fournisseurs de SIEM sur le marché. Les clients ayant besoin de services SIEM gérés ou cogérés doivent s'assurer que le fournisseur choisi peut prendre en charge le SIEM Devo et créer du contenu personnalisé supplémentaire pour améliorer les règles fournies par Devo.

Elastic

Elastic est un Visionnaire de ce Magic Quadrant. Sa solution Elastic Security est principalement axée sur l'analyse de la sécurité et la fonctionnalité de recherche d'entreprise associée à l'agent de sécurité Elastic Endpoint, qui est inclus dans la solution SIEM. La majorité des clients Elastic Security se trouvent en Amérique du Nord et en Europe, avec une répartition égale entre petites, moyennes et grandes entreprises. La croissance des nouveaux clients est actuellement plus élevée parmi les petites organisations. En 2021, Elastic a finalisé l'acquisition de Cmd et build security pour offrir une fonctionnalité de plateforme de protection des workloads cloud au sein de l'agent Elastic inclus avec Elastic Security. Les licences sont basées sur des ressources cloud telles que le calcul et le stockage pour prendre en charge l'environnement client.

Points forts

- **Visualisation personnalisée :** Elastic est connu pour ses tableaux de bord hautement personnalisables et la création de vues préférentielles des données à des fins d'analyse. Les utilisateurs peuvent utiliser les fonctionnalités combinées d'observabilité et de sécurité au sein d'une même vue pour obtenir des vues uniques de la chronologie et des activités adjacentes.

- **Fonctionnalité de recherche :** Elastic Security utilise sa capacité de recherche populaire et son langage de requête, qui est également utilisé comme moteur de recherche et de requête back-end par d'autres fournisseurs de SIEM, pour faciliter les tâches d'opérations de sécurité telles que la chasse aux menaces. La capacité d'Elastic à analyser et indexer pratiquement n'importe quelle partie d'un log donne aux

opérateurs de sécurité des options illimitées pour rechercher et découper les données qui ont été indexées.

- **Intégrations de collaboration et de notification** : Elastic utilise des actions et des connecteurs pour s'intégrer à plusieurs outils de collaboration, systèmes de tickets et outils de notification. Les acheteurs à la recherche d'un SIEM pouvant s'intégrer à leur outil de collaboration pour les incidents de prédilection constateront qu'Elastic Security prend en charge l'intégration à de nombreuses solutions tierces populaires.

Réserves

- **Fonctions SIEM modernes natives** : Elastic Security n'offre pas de SOAR natif dans sa solution SIEM, s'appuyant plutôt sur des intégrations partenaires avec d'autres fournisseurs SOAR et offrant certaines actions de réponse avec Elastic Agent. Aucune capacité TIP n'existe dans la solution, une fonctionnalité utilisée dans un nombre croissant de solutions concurrentes.

- **Prise en charge de l'EDR par des tiers** : Elastic Security prend en charge la collecte de données auprès des principaux fournisseurs EDR. Cependant, la prise en charge bidirectionnelle des fournisseurs EDR non élastiques doit être configurée à l'aide du connecteur REST générique d'Elastic.

- **Rapports de conformité** : Elastic Security ne prend pas en charge les alertes et les rapports sur les normes de conformité. Les acheteurs devront trouver des solutions alternatives pour le reporting de conformité.

Exabeam

Exabeam est un Leader de ce Magic Quadrant. La solution SIEM SaaS d'Exabeam, SIEM Exabeam Fusion, est disponible en tant que produit de base ou groupée avec les versions d'entreprise. Ces produits sont également disponibles pour le cloud hybride. La version entreprise comprend Advanced Analytics, Threat Hunter, Entity Analytics et Case Manager. Un stockage de données cloud supplémentaire (Cloud Archive) et un répondeur d'incident (SOAR) sont disponibles en tant que modules complémentaires. La majorité des clients d'Exabeam se trouvent en Amérique du Nord, puis en Europe. La plupart des clients sont de grandes entreprises, mais les volumes de clients de taille moyenne et plus petite augmentent. La licence est basée sur la durée et dépend des volumes de données ingérés.

Points forts

- **Stockage des journaux consultable à long terme** : La combinaison d'Exabeam Cloud Archive (pour une conservation des données jusqu'à 10 ans), la recherche d'événements normalisés, d'anomalies, d'indicateurs de compromission et d'une chronologie d'événements de logs avec enrichissement automatisé permet des détections et des investigations soutenues par un contexte riche sur de longues périodes.

- **Accès en direct aux données de tiers** : Exabeam Fusion SIEM est capable d'afficher et de traiter les données en direct provenant de systèmes tiers (tels que les flux de threat intelligence), ce qui permet au SIEM de fonctionner de manière plus décentralisée pour certains scénarios d'utilisation. La décentralisation des données permet des déploiements plus rentables, avec des données plus récentes, ce qui devrait être une tendance clé pour le SIEM au cours des 18 prochains mois.

- **Hiérarchisation efficace des alertes** : la notation dynamique permet aux clients de faire ressortir les découvertes à fort intérêt provenant d'alertes tierces (en plus des propres alertes d'Exabeam) à l'aide de

modèles de contextualisation et d'analyse en temps réel. Cela permet aux analystes de sécurité d'obtenir une vue prioritaire de toutes les alertes générées sur l'ensemble de leur pile technologique de sécurité.

Réserves

- **Manque de composants de l'écosystème natif** : Exabeam s'appuie sur des EDR et NDR tiers. Cette absence de fonctionnalité native place Exabeam derrière certains concurrents du marché sur ce point et réduit sa capacité à répondre nativement aux menaces sans investir davantage dans des ensembles d'outils compatibles.
- **Communication confuse autour de Fusion XDR et de Fusion SIEM :** Exabeam est à cheval sur ces deux marchés dans son marketing et le manque de cohérence dans la dénomination et la fonctionnalité des produits a été un sujet de discorde pour les utilisateurs finaux.
- **Temps d'intégration prolongé :** le SIEM Exabeam nécessite un plus grand nombre de jours de services professionnels pour être configuré que les autres SIEM SaaS sur le marché. Cela entraîne des frais et une complexité supplémentaires pour les utilisateurs finaux. De nombreux kits de services professionnels sont disponibles.

Fortinet

Fortinet est un Challenger de ce Magic Quadrant. Sa solution SIEM est FortiSIEM. Fortinet a une présence mondiale et des clients dans toutes les principales régions du monde, mais en particulier en Amérique du Nord et en Europe. Ce produit inclut des agents avancés (pour UEBA basée sur Windows). FortiSIEM s'intègre à FortiSOAR, FortiAnalyzer et à d'autres éléments de la suite de produits de sécurité de Fortinet. La tarification est basée sur les appareils pour SOAR, EPS et le nombre d'agents pour SIEM. FortiSIEM est disponible en tant qu'appliance virtuelle ou physique. La licence est basée sur les périphériques associés à 10 événements par seconde par périphérique. Des licences perpétuelles et des licences par abonnement sont disponibles.

Points forts

- **Assistance pour les prestataires de services et les organisations complexes** : Fortinet FortiSIEM offre une prise en charge multi-entités intégrée pour les organisations complexes et les fournisseurs de services, ainsi qu'une variété de fonctionnalités qui leur sont spécifiques. Il propose également un modèle basé sur la consommation pour les fournisseurs de services de sécurité gérés (managed security service providers, MSSP) avec un EPS illimité.
- **Capacités natives de visibilité des actifs :** Fortinet FortiSIEM dispose d'une fonction de découverte des actifs puissante et d'une base de données de gestion de la configuration (configuration management database, CMDB) intégrée. Cela fournit une visibilité centralisée des actifs découverts via une analyse active et une inspection passive des logs.
- **Intégration à l'écosystème Fortinet au sens large** : Fortinet propose un écosystème diversifié de produits de sécurité et de réseau intégrés via Fortinet Security Fabric. Les clients potentiels et existants de Fortinet à la recherche d'un fournisseur unique pour leur fournir des solutions de supervision, de détection et de réponse aux menaces doivent envisager Fortinet.

Réserves

- **Absence de stratégie directe en tant que service** : Fortinet s'appuie sur des partenaires qui offrent des services d'hébergement pour FortiSIEM comme moyen de fournir une expérience de type SaaS aux

acheteurs. Les organisations d'utilisateurs finaux peuvent déployer la solution dans leur propre cloud public ou privé, ou en tant que modèle de cloud hybride.

- **Couverture limitée pour la supervision des environnements cloud** : la couverture de sécurité cloud de FortiSIEM n'est pas aussi robuste que celle des autres concurrents. Il ne prend pas en charge plusieurs services d'infrastructure et de plateforme de cloud public (cloud infrastructure and platform services, CIPS), et les seuls courtiers de sécurité d'accès au cloud (cloud access security brokers, CASB) pris en charge sont FortiCASB de Fortinet et Oracle CASB.

- **Options d'analyse du comportement des utilisateurs et des entités** : UEBA est disponible en deux versions : une offre premium et une version plus limitée native de FortiSIEM. Les deux nécessitent le déploiement d'agents et manquent de fonctions disponibles chez les concurrents, telles que la possibilité de créer des groupes de pairs dynamiques. Cependant, le plan d'action de Fortinet indique que ces lacunes seront traitées.

Gurucul

Gurucul est un Visionnaire de ce Magic Quadrant. Son SIEM s'appelle Analytics-Driven SIEM. Il s'agit d'une solution modulaire largement axée sur le SIEM, l'UEBA, l'analytique d'identité, l'analyse de la fraude, le SOAR et l'analyse du trafic réseau. Gurucul propose une fonctionnalité TDIR intégrée via sa plateforme Security Analytics and Operations. La présence de la société sur le marché est principalement nord-américaine et son profil client est largement basé sur les grandes entreprises. Gurucul dispose d'un plan d'action robuste qui s'étend à l'intégration des réseaux sociaux, à l'intégration de l'évaluation de la posture de sécurité et à l'intégration améliorée avec les services de threat intelligence et de protection contre les risques numériques. La licence est basée sur des actifs supervisés et est disponible sous forme d'abonnement ou perpétuelle.

Points forts

- **Prise en charge de l'architecture et du lac de données** : Gurucul prend en charge un modèle d'apport de votre propre lac de données et/ou d'entrepôt, ce qui évite de devoir répliquer les données dans un autre magasin de données pour des raisons de sécurité. Gurucul propose une large gamme d'options d'architecture pour prendre en charge les modèles SaaS et déployables par le client.

- **Modèles de machine learning communautaires et contenu sur les menaces** : les détections ouvertes dans la bibliothèque de détection des menaces de Gurucul sont à la disposition de tous les utilisateurs pour le feedback et le partage, ce qui permet de personnaliser et de partager des informations sur les variations des algorithmes et du contenu des menaces pour modifier les détections.

- **Tarification prévisible** : Gurucul tarife sa solution en fonction des actifs, ce qui soulage les préoccupations concernant les dépassements de volume de données ou de vitesse, et il n'y a aucune limitation de stockage. Il offre une structure modulaire permettant aux acheteurs de sélectionner uniquement les fonctionnalités dont ils ont besoin pour leur environnement particulier.

Réserves

- **Fonctionnalités limitées de threat intelligence** : Gurucul n'offre pas les mêmes fonctionnalités de plateforme/gestion de threat intelligence que certains concurrents. Les acheteurs qui ont besoin de fonctions de threat intelligence (comme l'analyse des liens, le marquage personnalisé et la gestion des indicateurs) ne retrouveront pas ces fonctionnalités dans Gurucul.

- **Présence sur le marché et exécution commerciale :** Gurucul reste relativement inconnu sur le marché du SIEM malgré des efforts marketing accrus. Les acheteurs de SIEM ne connaissent souvent pas Gurucul ou ses solutions, et il y a un manque de services de sécurité gérés prenant en charge les déploiements cogérés de Gurucul par rapport aux autres fournisseurs de SIEM.

- **Accent mis sur les grands environnements :** l'écrasante majorité des clients Gurucul sont des grandes entreprises, qui disposent souvent d'importantes équipes de sécurité matures, nécessaires pour tirer parti d'un SIEM de sécurité complexe comme le SIEM axé sur l'analytique. Gurucul offre une solution multifacettes nécessitant une plus grande expérience en analyse de données et opérations de sécurité.

Huawei

Huawei est un Acteur de niche de ce Magic Quadrant. Sa solution SIEM s'appelle HiSec Insight et comprend Huawei Cloud Security Brain. Il existe de nombreux modules supplémentaires et technologies complémentaires pour répondre aux exigences spécifiques aux fonctionnalités ou à l'architecture. Ses clients SIEM sont largement concentrés en Chine, bien qu'un certain nombre de clients soit basé au Moyen-Orient, en Afrique et en Amérique latine. Sa clientèle est répartie presque uniformément entre les grandes et moyennes entreprises, mais il existe également des clients plus petits. La tarification des déploiements sur site est basée sur la vitesse des données (EPS) et le volume (gigaoctets par jour), avec des frais supplémentaires pour la conservation des logs et les modules complémentaires. Les déploiements SaaS sont basés sur le nombre de serveurs Elastic CloudServers achetés.

Points forts

- **Analyse comportementale :** l'analyse est un domaine dans lequel Huawei a investi. Ses analyses du comportement des utilisateurs fournissent des détections dynamiques basées sur des groupes de pairs. Son classement des risques basé sur le machine learning pour les entités reflète des facteurs tels que la valeur des actifs, les détections basées sur des règles associées et les données de vulnérabilité.

- **Écosystème de produits étendu :** Huawei propose un certain nombre de fonctionnalités intégrées, notamment la détection et la réponse au niveau du réseau, le sandboxing, la déception, l'analyse du comportement de l'utilisateur, l'orchestration et la réponse, et la threat intelligence.

- **Flexibilité par rapport aux facteurs de forme :** le produit Huawei est disponible en plusieurs formats qui peuvent être mélangés selon les besoins. Il s'agit notamment d'appliances logicielles, physiques et virtuelles. Il existe également des options d'hébergement sur l'infrastructure de cloud public ou privé de Huawei.

Réserves

- **Prise en charge limitée de la supervision de l'infrastructure cloud** : la supervision des infrastructures cloud est limitée au propre cloud de Huawei. Aucun autre service cloud n'est pris en charge d'emblée.

- **Manque de prise en charge de la supervision SaaS** : la supervision prête à l'emploi des applications SaaS populaires n'est pas fournie. La plateforme de Huawei ne dispose pas d'intégrations avec Microsoft 365, Google Workspace ou les applications de Workday, Salesforce ou Box.

- **Disponibilité limitée :** l'accent mis par Huawei sur la Chine, les marchés émergents en Asie/Pacifique, ainsi que le Moyen-Orient et l'Afrique signifie que son produit n'est pas exposé aux acheteurs de SIEM ailleurs. Huawei ne prévoit pas d'expansion immédiate en Amérique du Nord ou en Europe.

IBM

IBM est un Leader de ce Magic Quadrant. Son produit IBM QRadar peut être déployé via un logiciel sur site, dans un cloud public/privé ou hybride, ou livré dans un format cloud natif sous le nom de QRadar on Cloud (QROC). La clientèle SIEM d'IBM couvre l'Amérique du Nord, l'Europe, l'Asie/Pacifique, le Moyen-Orient et l'Amérique latine, la majorité d'entre eux étant des clients de taille moyenne et des entreprises. En plus de QRadar, IBM propose d'autres produits de sécurité tels que QRadar Network Insights, QRadar Vulnerability Manager, QRadar XDR Connect, QRadar SOAR (anciennement Resilient) et Cloud Pak for Security (CP4S). La licence pour QRadar SIEM est basée sur les événements par seconde (EPS) et/ou les flux par minute (FPM). Une licence illimitée basée sur serveur est une solution alternative pour les instances déployées dans le cloud uniquement.

Points forts

- **Analyse et personnalisation solides** : QRadar dispose d'un grand nombre de contenus prêts à l'emploi et de capacités analytiques. Les clients ont également formulé des retours positifs sur la capacité de QRadar à créer et personnaliser des applications et des tableaux de bord.
- **Importante activité et présence dans le domaine de la sécurité** : IBM dispose de la portée mondiale requise (via des canaux directs et partenaires) pour fournir ses produits, son support et ses services dans toutes les principales régions géographiques. De plus, il dispose de nombreux membres du personnel qui comprennent les réglementations spécifiques à chaque région et parlent plusieurs langues afin de prendre en charge des projets et des configurations personnalisés.
- **Plusieurs offres de produits de sécurité** : IBM propose une large gamme de technologies complémentaires facultatives et étroitement intégrées, ainsi que des services pour compléter et prendre en charge QRadar. Il s'agit notamment de la sécurité réseau, de la gestion des vulnérabilités, de la threat intelligence, de la protection des données, des services UEBA, SOAR et MSS/MDR.

Réserves

- **Les règles de corrélation et l'analyse sont analogues** : QROC ne fait pas la distinction entre les règles de corrélation et l'analyse ; par conséquent, il existe différents degrés de complexité, de simple à avancé, en ce qui concerne le contenu prêt à l'emploi, ce qui rend la comparaison difficile.
- **Cloud Pak ralentit l'innovation SIEM** : l'innovation de QRadar SIEM a été lente, IBM transférant les ressources vers la plateforme Cloud Pak for Security et les capacités de sécurité de nouvelle génération.
- **Les mises en œuvre justifient une amélioration** : sur la base des commentaires, les clients ont signalé que le déploiement initial peut être un processus complexe. Il peut également manquer de flexibilité en termes d'intégration de nouvelles sources de données.

Logpoint

LogPoint est un Acteur de niche de ce Magic Quadrant. Sa solution SIEM est combinée nativement avec la fonctionnalité SOAR et est principalement utilisée par les clients dans un format SaaS ou basés sur le cloud. La plus grande concentration d'acheteurs est constituée de clients de petite et moyenne taille basés en Europe. LogPoint dispose d'une offre remarquable pour la supervision et la réaction aux menaces pesant sur les plateformes SAP. La licence est basée sur le nombre de « nœuds » supervisés. Le composant SOAR est mesuré par le nombre d'utilisateurs, avec une licence utilisateur unique incluse avec le produit SIEM. Les fonctionnalités UEBA sont concédées sous licence séparément.

Points forts

- **Tarification simple et facile à comprendre :** LogPoint propose un modèle de tarification parmi les plus faciles à comprendre sur le marché. Une tarification échelonnée basée sur le nombre de « nœuds » (ou d'actifs) envoyant des journaux à la solution est disponible pour l'élément SIEM principal du produit, le SOAR groupé étant tarifé par le nombre d'utilisateurs (une licence à utilisateur unique est incluse avec le produit SIEM).

- **Supervision des applications SaaS tierces :** l'accent mis sur les plateformes SaaS tierces fait clairement partie de la stratégie de LogPoint, avec des capacités significatives pour SAP et Salesforce, et une bonne prise en charge de Microsoft 365. Des intégrations pour le service S3 d'Amazon et ServiceNow sont également disponibles.

- **Assistance et support :** l'offre SIEM + SOAR de LogPoint propose des offres de services complémentaires pour soutenir la supervision opérationnelle du SIEM et la conception et le développement des playbooks SOAR. Ils sont disponibles moyennant un abonnement supplémentaire directement auprès de LogPoint.

Réserves

- **Manque de personnalisation des analyses :** LogPoint prend en charge un certain nombre d'ensembles d'outils qui ont la capacité de fournir du contenu analytique et, bien qu'un grand nombre d'analyses prêtes à l'emploi soient disponibles, les utilisateurs avancés ne pourront pas les personnaliser eux-mêmes.

- **Stockage SIEM SaaS limité :** LogPoint inclut 90 jours de stockage de journaux indexés avec son produit SaaS. 90 jours supplémentaires de stockage « à froid » sont facturables, et des périodes de stockage plus longues n'apparaissent pas sur les listes de prix. Les acheteurs potentiels doivent se renseigner sur le coût du stockage à long terme. Le déchargement vers le stockage de logs tiers est disponible.

- **Centré sur l'Europe :** LogPoint sert principalement des clients dans une région, l'Europe. Bien que le nombre de ventes en Amérique du Nord soit manifestement limité, des infrastructures et des forces de vente semblent être présentes dans la région et sont en croissance. Les acheteurs doivent s'assurer que le niveau d'assistance internationale dont ils ont besoin est disponible.

LogRhythm

LogRhythm est un Challenger de ce Magic Quadrant. Sa solution SIEM est la plateforme SIEM LogRhythm, qui comprend plusieurs composants complémentaires pour fournir des analyses des terminaux, du réseau et du comportement des utilisateurs. Une grande majorité de ses clients SIEM se trouvent en Amérique du Nord et en Europe, le reste étant situé en Asie/Pacifique, au Moyen-Orient, en Afrique et en Amérique latine. Sa clientèle se compose essentiellement de petites et moyennes entreprises, bien que de grandes entreprises aient également acheté le SIEM de LogRhythm. Une option cloud est disponible, mais la plupart des clients ont déployé leur SIEM sur site. Les licences sont disponibles à durée indéfinie (tarifées en fonction du nombre moyen de messages par seconde et par jour) ou sur la base d'un abonnement (tarifé en fonction du nombre d'employés).

Points forts

- **Présence étendue des revendeurs :** LogRhythm dispose d'une équipe solide de partenaires revendeurs dans toutes les grandes régions du monde. Cette force est reflétée par le large soutien des fournisseurs de services gérés pour aider les acheteurs disposant de ressources modestes à gérer et superviser leur SIEM.

- **Options de pilote et de preuve de concept (proof of concept, POC) :** les acheteurs peuvent tirer parti de plusieurs types de programmes pilotes et POC, allant d'ateliers de préparation à des exercices d'essai hébergés et basés sur des scénarios, en passant par des options « essayer et acheter ».

- **Workflow d'investigation et de gestion des cas :** LogRhythm fournit des fonctionnalités avancées et évoluées d'investigation et de gestion des cas qui assemblent le contexte et permettent aux utilisateurs de créer une base de preuves pour le traitement des cas.

Réserves

- **Options limitées basées sur le cloud :** les récentes acquisitions et le plan d'action des produits de LogRhythm témoignent des progrès réalisés dans le développement initial de ses capacités SaaS SIEM, mais le fournisseur est à la traîne par rapport à de nombreux concurrents à cet égard. L'offre SIEM cloud offre des interfaces fractionnées qui obligent les utilisateurs à basculer entre deux environnements. Les fonctions administratives utilisent l'ancienne console d'administration LogRhythm pour créer des analyses et des règles, et pour gérer les flux de threat intelligence. Le tableau de bord et l'interface utilisateur des alertes sont plus alignés sur ce que les utilisateurs qualifieraient de cloud-natives.

- **L'App Store est un défi :** le magasin d'applications LogRhythms est proposé dans l'ancienne application de console d'administration Knowledge Base. Il ne dispose que de fonctionnalités de base et ne ressemble pas à une librairie applicative SaaS moderne, où les utilisateurs peuvent utiliser des intégrations de clés API pour ajouter facilement des solutions ponctuelles ou des sources de données (comme c'est le cas de certaines solutions concurrentes).

- **Passage au cloud :** LogRhythm est confronté au défi de développer un nouveau SIEM basé sur le cloud et de présenter ses capacités aux acheteurs, tout en maintenant son SIEM hérité et en exécutant ses plans de migration des clients vers la nouvelle architecture SaaS.

ManageEngine

ManageEngine est un Acteur de niche de ce Magic Quadrant. Sa solution SIEM Log360 est basée sur le cloud et déployée dans le datacenter de Zoho Corporation. Les principaux acheteurs de Log360 sont des moyennes et grandes entreprises situées principalement en Amérique du Nord, en Europe, au Moyen-Orient et en Asie/Pacifique. Outre son outil SIEM, Log360 comprend d'autres produits de sécurité tels que Firewall Analyzer, EventlLog Analyzer, ADAudit Plus, Vulnerability Manager Plus, Cloud Security Plus, DataSecurity Plus et FileAnalysis. Les licences SaaS sont basées sur la quantité de données stockée dans le cloud sur une période spécifique. La licence de la version sur site est basée sur le nombre de sources de logs. Cela inclut les périphériques tels que les postes de travail, les serveurs Windows et autres périphériques réseau. Des fonctionnalités telles que l'analyse du comportement des utilisateurs et des entités (UEBA), l'analyse avancée des menaces et l'audit des applications sont disponibles en tant que modules complémentaires.

Points forts

- **Capacités de sécurité du cloud :** ManageEngine propose désormais des fonctionnalités CASB, accessibles via Log360 Cloud. Cela permet d'enrichir la solution SIEM Log360, ainsi que de détecter les applications cloud non autorisées et d'arrêter l'utilisation des applications interdites.

- **Facilité de mise en œuvre et d'exploitation :** les évaluations sur les Peer Insights de Gartner concernant la capacité de ManageEngine à déployer et utiliser facilement l'outil SIEM sont généralement positives.

- **Fonctionnalités natives de confidentialité et de protection des données :** ManageEngine fournit des capacités de chiffrement, de masquage et d'obscurcissement des données, qui s'alignent sur les

exigences de confidentialité et de protection des données du Règlement général sur la protection des données (RGPD).

Réserves

- **Manque de capacités avancées :** ManageEngine manque de capacités plus avancées qui seraient très probablement nécessaires et exigées par des organisations plus développées, telles que l'analyse avancée (analyses ML et deep learning supervisées, par exemple) et le SOAR natif.
- **Intégrations limitées avec des solutions tierces :** le produit Log360 de ManageEngine dispose d'intégrations bidirectionnelles limitées avec des outils de sécurité tiers, tels qu'EDR, NDR et SOAR.
- **Limitations de l'interface utilisateur :** bien que Log360 prenne en charge les intégrations avec les principaux outils ITSM et dispose de sa propre fonctionnalité de chat, il n'affiche pas d'informations provenant de systèmes tiers et ne peut pas partager de contenu (comme des rapports) entre les utilisateurs.

Micro Focus

Micro Focus est un Visionnaire de ce Magic Quadrant. Son produit ArcSight est principalement axé sur les fonctionnalités SIEM, UEBA, SOAR et TIP. Les opérations d'ArcSight sont géographiquement diversifiées (à l'exception de l'Amérique latine) et son profil client est principalement de taille moyenne. Les déploiements sur site l'emportent de loin sur les déploiements cloud-natifs, largement attribués à la disponibilité récente de son option cloud. Micro Focus a investi massivement dans son portefeuille de produits de sécurité CyberRes qui comprend la sécurité des données, la gestion de l'accès aux identités (identity access management, IAM), la sécurité des applications et les opérations de sécurité. Le premier produit phare du portefeuille d'opérations de sécurité CyberRes est Galaxy, une solution cloud-native de threat intelligence qui s'intègre au workflow ArcSight. La licence est basée sur l'EPS pour SIEM et par entité pour UEBA.

Points forts

- **Plateforme de threat intelligence (Threat intelligence platform, TIP) :** la solution Galaxy Threat Acceleration Plus (GTAP) Basic TIP est incluse avec ArcSight SIEM. Elle fournit des informations open source MISP à tous les acheteurs ArcSight sans frais supplémentaires et peut être mise à niveau vers GTAP Plus, qui fournit des flux de threat intelligence premium CyberRes. Cette solution SaaS TIP fournit une vue graphique et une analyse des liens entre les indicateurs.
- **SOAR inclus avec le SIEM :** ArcSight SIEM inclut SOAR sans frais supplémentaires, mais il ne s'agit pas encore d'une fonctionnalité SaaS. Les utilisateurs peuvent utiliser un espace graphique pour créer des workflows avec une pléthore d'options de configuration présentées sous forme de listes déroulantes. Les ingénieurs en automatisation peuvent également utiliser une interface de développement basée sur le code pour créer des playbooks plus complexes. Toutes les actions de réponse automatisées sont enregistrées dans un fichier de gestion des cas.
- **Interface utilisateur ArcSight Fusion :** l'interface utilisateur Fusion fournit une interface mise à jour avec une sensation SaaS, indiquant un écart par rapport à l'interface utilisateur historique de la console ArcSight. Fusion fournit un calendrier moderne et des vues graphiques des données pour montrer les modèles d'activité d'un utilisateur ou d'une entité. Les analystes peuvent utiliser un curseur pour filtrer les événements en fonction du risque afin de restreindre l'activité d'une investigation.

Réserves

- **Interface utilisateur divisée entre ArcSight Console et SaaS :** les utilisateurs découvriront qu'il est toujours nécessaire de se tourner vers l'interface utilisateur fonctionnelle, mais plus ancienne de la console ArcSight pour la fonctionnalité de gestion, même dans l'architecture SaaS. FlexConnector, Quick Flex, FlexAgent, Correlation Condition Editor (CCE) sont tous des exemples où l'ancienne console ArcSight est toujours requise par rapport à l'utilisation de l'interface utilisateur Fusion mise à jour.

- **La personnalisation/création d'analyses nécessite des outils externes :** ArcSight ne fournit pas d'interface utilisateur pour la prise en charge du modèle de machine learning personnalisé. Au lieu de cela, les utilisateurs utilisent des outils de science des données tiers (tels que SPSS, SAS ou R) pour exporter des modèles dans un format PMML standard. Ces modèles peuvent ensuite être importés dans ArcSight. Bien que cela élimine le fardeau de devoir apprendre à maîtriser une interface d'analyse et un workflow spécifiques à ArcSight, l'utilisation d'outils externes peut ne pas être aussi intuitive ou conviviale pour certains acheteurs.

- **Options d'affichage des événements associés :** Micro Focus n'a démontré que deux options pour afficher les événements associés à un incident découvert dans ArcSight. La méthode principale est l'interface native de gestion des incidents (SOAR) d'ArcSight, et la seconde méthode consiste à télécharger un fichier PDF. Certains acheteurs peuvent souhaiter des options supplémentaires pour faciliter les workflows d'investigation. Les acheteurs devront contacter Micro Focus pour obtenir des conseils et des options supplémentaires.

Microsoft

Microsoft est un Leader de ce Magic Quadrant. Son produit SIEM, Microsoft Sentinel, est fourni uniquement en tant que SaaS via les centres de données Azure de Microsoft. Microsoft dispose d'une base de clients importante et diversifiée, qui s'adresse aussi bien aux grands qu'aux petits clients, et qui propose le produit SIEM dans plusieurs contextes à l'échelle internationale. La licence est basée sur le volume de données ingérées, via une capacité réservée ou le paiement à l'utilisation. Cependant, de nombreux niveaux d'entreprise Microsoft pour Microsoft 365 incluent des crédits pour l'utilisation de Sentinel et Defender. Un stockage de données amélioré, des capacités complémentaires de l'écosystème Microsoft (telles que Defender for Endpoint et Defender for IoT) sont disponibles à un coût supplémentaire.

Points forts

- **Écosystème riche de produits de sécurité hautement intégrés :** Microsoft fournit intrinsèquement un grand nombre de produits d'écosystème hautement intégrés dans des domaines tels que la sécurité CASB, l'identité, les points de terminaison, le réseau et les technologies opérationnelles. De plus, un certain nombre de ses capacités informatiques traditionnelles ont des intégrations bidirectionnelles. Les acheteurs qui investissent dans un large éventail de produits Microsoft, à la fois de sécurité et sans lien avec la sécurité, peuvent s'attendre à une excellente visibilité de la sécurité sur l'ensemble de leur parc.

- **Roadmap en développement rapide :** les clients qui investissent dans Microsoft Sentinel ont déjà constaté une augmentation significative et continue des fonctionnalités, de la facilité d'utilisation et de la croissance des communautés d'utilisateurs finaux au cours de la période de leur investissement.

- **Opérations hiérarchisées et hybrides :** la capacité à configurer, gérer et superviser de manière cohérente plusieurs instances Sentinel combinées à l'aide de la fonctionnalité « Lighthouse » profite à la fois aux utilisateurs disposant d'environnements complexes et à ceux qui utilisent Sentinel et souhaitent passer à un modèle de services gérés avec Microsoft directement ou avec l'un des partenaires de services gérés de plus en plus nombreux sur le marché.

Réserves

- **Difficulté à comprendre le coût réel :** bien que la tarification utilise un modèle simple d'ingestion de données pour la tarification et dispose d'options de paiement à l'utilisation, les clients indiquent que la tarification est imprévisible et complexe à comprendre lorsqu'elle est associée à d'autres licences Microsoft. Les acheteurs qui envisagent Sentinel doivent prendre en compte le coût du déplacement des données de leurs actifs cloud sur site et tiers, ainsi que le prix du SIEM.

- **Potentiel de blocage indirect du fournisseur :** l'intégration des produits Microsoft dans Sentinel est facile à mettre en œuvre, cependant, il est difficile de comparer les fonctionnalités et les prix natifs de Microsoft avec des intégrations tierces. Les acheteurs doivent planifier soigneusement leur sélection d'outils SOC et s'assurer que leur dépendance à l'égard d'un fournisseur n'affecte pas leur capacité à atteindre leurs objectifs.

- **Contenu prêt à l'emploi limité :** par rapport à de nombreux autres produits de SIEM, Sentinel manque de fonctionnalités prêtes à l'emploi, y compris le reporting de conformité. Cependant, les clients ont la flexibilité de créer leur propre contenu analytique, ce qui est moins courant sur l'ensemble du marché. Les acheteurs doivent prendre en compte les dépenses supplémentaires des services professionnels nécessaires pour soutenir la livraison de leurs besoins lors de l'évaluation du coût réel.

Rapid7

Rapid7 est un Challenger de ce Magic Quadrant. Sa solution SIEM, InsightIDR, fonctionne sur la plateforme Insight, basée sur le cloud. Les autres produits disponibles comprennent InsightVM (gestion des vulnérabilités), InsightAppSec, InsightConnect (SOAR), InsightCloudSec (gestion de la posture de sécurité du cloud) et Threat Command (threat intelligence). Les clients du SIEM d'InsightIDR sont surtout concentrés aux États-Unis, suivis par l'Europe et l'Asie-Pacifique. La licence est basée sur une licence à durée déterminée, avec un modèle de tarification simple basé sur le nombre d'actifs supervisés.

Points forts

- **Large gamme de capacités intégrées** : Rapid7 offre un SIEM de base avec une multitude de capacités de sécurité, y compris InsightVM, qui offre une gestion des vulnérabilités ; et InsightIDR, qui dispose de capacités EDR, UEBA et NDR. Toutes ces capacités sont hautement intégrées les unes aux autres pour offrir une expérience unique pour les opérateurs SOC.

- **Rentable :** Rapid7 fait partie des solutions les plus rentables évaluées dans le cadre de cette étude, avec un prix moyen pour son SIEM SaaS principal bien inférieur à la moyenne du marché.

- **Service de gestion de la détection et de la réponse :** elle est disponible directement auprès de Rapid7 moyennant un coût supplémentaire. Il s'agit d'une source unique pour les clients qui souhaitent accéder au produit SIEM et qui ont besoin d'un service d'assistance pour la supervision et l'investigation.

Réserves

- **Aucune compatibilité avec le stockage de données tiers :** le produit SIEM de Rapid7 ne prend pas ou peu en charge le rappel des données du stockage tiers. Cela peut entraîner des coûts supplémentaires et une augmentation des besoins réglementaires. Les acheteurs ayant des exigences de stockage de grande envergure, ou des besoins spécifiques concernant la résidence régionale des données, doivent s'assurer que Rapid7 peut répondre à leurs exigences dans ces domaines.

- **Maintenance des intégrations d'automatisation tierces :** Rapid7 n'a pas d'intégrations disponibles sur le marché pour les plateformes SOAR/d'automatisation tierces. Les acheteurs qui ont déjà investi dans ces outils doivent tenir compte des frais de maintenance liés à l'intégration ou à l'utilisation conjointe de ces produits dans le cadre de leur ensemble technologique d'opérations de sécurité.

- **Manque de soutien pour l'obscurcissement des données :** la solution de Rapid7 n'est pas en mesure de prendre en charge l'obscurcissement natif des données, ce qui signifie que les données stockées sur la plateforme peuvent ne pas respecter certaines normes de confidentialité ou exigences de conformité localisées. L'acheteur doit s'engager auprès des équipes de services professionnels de Rapid7, ou éventuellement des solutions tierces, s'ils ont l'obligation de masquer les données de logs.

Securonix

Securonix est un Leader de ce Magic Quadrant. Sa solution SIEM est Next-Gen SIEM et comprend Next-Gen SIEM, Security Data Lake, UEBA, SOAR, NDR, la threat intelligence, l'analyse du comportement des adversaires et plusieurs applications spécifiques à un scénario d'utilisation (comme pour les soins de santé et SAP). La plupart des clients de Securonix se trouvent en Amérique du Nord, puis en Europe, en Asie/Pacifique, au Moyen-Orient et en Afrique, et en Amérique latine. Les clients sont principalement de grandes entreprises, mais ses produits attirent également certains clients de taille moyenne. Les clients de plus petite taille sont principalement servis par des partenaires de services gérés. La licence est basée sur les identités et l'EPS. La plupart des acheteurs optent pour des licences à durée déterminée, mais des licences perpétuelles sont disponibles.

Points forts

- **Accès au lac de données tiers :** Securonix SIEM est capable d'interroger et d'afficher des données en direct provenant de systèmes tiers tels que des lacs de données, permettant à la plateforme de fonctionner de manière plus décentralisée. La décentralisation des données permet des déploiements plus rentables, avec des données plus à jour, et devrait être une tendance clé pour le SIEM au cours des 18 prochains mois.

- **Accès à la threat intelligence inclus :** Securonix fournit un ensemble d'intégrations de threat intelligence pour un enrichissement supplémentaire sans frais additionnels. Elle a publié ces informations dans le domaine public pour utilisation.

- **Workflow et gestion des cas :** Securonix offre des capacités d'investigation et de gestion de cas évoluées qui assemblent le contexte et le partagent avec le contexte et la collaboration au sein de la plateforme.

Réserves

- **Chevauchement dans les messages marketing Open XDR et Next-Gen SIEM :** Securonix se situe à cheval sur les deux marchés dans son marketing. Assurez-vous donc de bien comprendre ce que vous attendez du produit avant de l'acheter.

- **Modèles de tarification non conventionnels :** Securonix utilise un modèle qui prend en compte à la fois l'EPS et les identités. Les utilisateurs doivent évaluer les exigences EPS pour éviter une augmentation inattendue des coûts. Les utilisateurs peuvent rencontrer des incohérences et des imprévisibilités dans les taux d'événements requis, et donc dans les coûts.

- **Offres d'analyses packagées supplémentaires :** Securonix dispose d'un ensemble complexe d'applications d'analyse premium dont le prix est fixé par utilisateur et par application. Lors de l'évaluation,

vous devez comprendre quelles fonctionnalités de l'application d'analyse sont déjà incluses, ou doivent être ajoutées pour obtenir une évaluation correcte. Bien que le coût d'achat de toutes les fonctionnalités soit similaire à celui d'un module complémentaire d'analyse unique d'autres fournisseurs de SIEM, il est difficile de comparer les offres, de se démarquer du marché et de planifier les capacités requises.

Splunk

Splunk est un Leader de ce Magic Quadrant. Son SIEM est Enterprise Security (Splunk ES) et est un complément à la solution Splunk Enterprise. Il est important de noter que Gartner n'évalue ni ne considère la solution de base Splunk Enterprise comme un SIEM. La majorité des acheteurs de Splunk ES sont basés en Amérique du Nord. Les principaux acheteurs de Splunk ES sont les grandes entreprises. La direction de Splunk ES est d'offrir plus d'enrichissement d'événements et d'artefacts grâce à son interface utilisateur, et de promouvoir la diffusion de plus de contenu. Des licences en fonction du volume de données indexées par jour ou des workloads cloud (désignées par le terme « Splunk Virtual Compute » ou unités de calcul virtuelles) sont disponibles.

Points forts

- **Fonctionnalités de sécurité intégrées :** Le modèle SaaS de Splunk ES comprend des fonctionnalités TIP et UEBA sans frais supplémentaires. Historiquement, Splunk utilise un modèle de produit modulaire pour vendre ses offres, mais propose désormais des composants critiques avec Splunk ES pour fournir une solution de sécurité plus complète.

- **Observabilité IT associée à la sécurité :** l'un des grands avantages de Splunk est sa capacité à fournir une observabilité et des analyses IT aux utilisateurs non spécialisés dans la sécurité, tout en offrant aux équipes de sécurité une fonctionnalité d'opérations de sécurité commune via Splunk ES. Splunk renforce la fusion des données environnementales avec la sécurité pour fournir aux utilisateurs une vue enrichie de leur environnement.

- **Expérience utilisateur de l'opération de sécurité :** les acheteurs de Splunk donnent constamment des retours positifs sur l'expérience utilisateur avec le produit ES via la fonctionnalité de requête, les capacités API, les tableaux de bord personnalisés et l'analyse basée sur la science des données prêts à l'emploi.

Réserves

- **Tarification :** les acheteurs continuent de faire part d'inquiétudes à l'égard des coûts de Splunk et la nouvelle tarification par unités de calcul virtuelles (Splunk Virtual Compute, SVC) n'a pas apporté le soulagement promis. Les demandes croissantes pour tout enregistrer obligent les clients existants de Splunk et les nouveaux acheteurs à envisager des alternatives moins chères pour compenser les coûts massifs d'ingestion et de stockage des données.

- **Complexité et expertise :** les acheteurs expriment une certaine inquiétude quant à la complexité de Splunk ES et les utilisateurs existants communiquent des problèmes de gestion des données au sein de la solution. Il existe également de réels problèmes de formation, de maintien et d'embauche d'experts de Splunk ES sur le marché en raison de la forte concurrence entre les propriétaires de Splunk ES pour le vivier de talents limité.

- **Expertise commerciale régionale :** la majorité de la force de vente de Splunk est basée en Amérique du Nord, avec un pourcentage non divulgué inférieur en dehors de la région. Le manque de compréhension des exigences et des restrictions d'autres marchés peut entraîner une mauvaise expérience d'un point de vue commercial et d'assistance.

Sumo Logic

Sumo Logic est un Visionnaire de ce Magic Quadrant. Son produit SIEM, Cloud SIEM, est fourni sous forme de solution SaaS uniquement. La base de clients de Sumo Logic est un mélange égal de petites, moyennes et grandes entreprises, la majorité étant basée en Amérique du Nord. La société a augmenté sa présence dans les régions Europe et Asie-Pacifique au cours de l'année passée. En 2021, Sumo Logic a acquis DFLabs, qui fournit des processus supplémentaires de gestion des incidents, des actions de playbook automatisées et un enrichissement via des sources d'informations externes avec une efficacité similaire à une offre SOAR autonome. La licence est basée sur un abonnement (avec une tarification basée sur l'ingestion de données) ou sur le crédit (avec des crédits utilisés pour permettre une utilisation spécifique des ressources, comme pour la recherche occasionnelle ou l'analyse continue), avec des options de tiering et d'offres groupées.

Points forts

- **SecOps et unification DevOps :** les utilisations de Sumo Logic peuvent s'étendre au-delà des scénarios d'utilisation des opérations de sécurité au développement et aux opérations, qui sont l'héritage de l'entreprise, et démocratisent les données pour plusieurs unités commerciales.
- **Threat intelligence commerciale gratuite prête à l'emploi :** Sumo Logic fournit de la threat intelligence via CrowdStrike pour un enrichissement supplémentaire sans accroissement des coûts
- **Fonctionnalité SOAR intégrée :** les capacités SOAR de DFLabs sont désormais assimilées à la post-acquisition de SIEM, ce qui réduit les tâches SecOps chronophages ainsi que le temps nécessaire pour déployer un SOAR, puis effectuer le travail d'intégration pour le rendre fonctionnel.

Réserves

- **Analyses avancées :** Sumo Logic ne dispose pas du même éventail de fonctionnalités d'analyse avancées, telles que l'UEBA, que certains de ses concurrents sur le marché du SIEM.
- **Expérience de recherche :** les évaluateurs de Peer Insights de Gartner ont exprimé leurs inquiétudes concernant les capacités de recherche de Sumo Logic, ayant notamment un impact sur les performances lors de la recherche de grands ensembles et/ou de données plus anciennes.
- **Visibilité limitée :** bien que Sumo Logic ait gagné en visibilité auprès des fournisseurs MSSP/MDR en termes de revendeurs et/ou de support SIEM géré, sa notoriété pour le SIEM auprès des utilisateurs finaux clients de Gartner reste faible.

Fournisseurs ajoutés et abandonnés

Nous révisons et ajustons nos critères d'inclusion aux différentes éditions du Magic Quadrant en fonction de l'évolution des marchés. En raison de ces ajustements, la liste des fournisseurs d'un Magic Quadrant peut varier au fil du temps. Le fait qu'un fournisseur apparaisse dans un Magic Quadrant une année et pas l'année suivante ne signifie pas nécessairement que nous avons changé d'avis à son sujet. Cela peut refléter une évolution du marché et, par conséquent, des critères d'évaluation, ou un changement d'orientation de la part de ce fournisseur.

Ajoutés

- Devo a satisfait aux exigences commerciales et fonctionnelles pour l'inclusion dans le Magic Quadrant 2022 pour le SIEM.

Abandonnés

- VenusTech n’a pas satisfait aux exigences fonctionnelles et commerciales pour figurer dans le Magic Quadrant 2022 pour le SIEM.
- FireEye s’est associé à McAfee via l’acquisition pour former Trellix et n’a pas satisfait aux exigences commerciales pour figurer dans le Magic Quadrant 2022 pour le SIEM.
- McAfee s’est associé à FireEye via l’acquisition pour former Trellix et n’a pas satisfait aux exigences commerciales pour figurer dans le Magic Quadrant 2022 pour le SIEM.
- Odyssey n’a pas satisfait aux exigences commerciales pour figurer dans le Magic Quadrant 2022 pour le SIEM.
- Netwitness, une société de RSA, n’a pas satisfait aux exigences fonctionnelles et commerciales pour figurer dans le Magic Quadrant 2022 pour le SIEM.

Critères d’inclusion et d’exclusion

Les critères d’inclusion représentent les attributs spécifiques que les analystes de Gartner considéraient nécessaires pour qu’un fournisseur puisse être inclus dans ce Magic Quadrant.

Pour être admissible à l’inclusion, un fournisseur devait remplir les critères suivants :

- Un produit qui fournit des capacités SIM et SEM aux clients utilisateurs finaux via un logiciel cloud-natif et/ou SaaS.
- Caractéristiques, fonctionnalités et solutions complémentaires comprenant au moins deux des capacités supplémentaires mentionnées ci-dessous, généralement disponibles, appartenant au fournisseur (entièrement acquises ou construites organiquement) et incluses dans le produit SIEM ou vendues en tant que modules complémentaires distincts au 1er février 2022.
  - Orchestration de la sécurité, automatisation et réponse (SOAR)
  - Plateforme de threat intelligence (TIP)
  - Analyse du comportement des utilisateurs et des entités (UEBA)
  - Stockage et reporting des données à long terme (plus de 365 jours)
- Un produit qui prend en charge la capture et l’analyse de données provenant de sources tierces hétérogènes via une API, en plus du flux de données ou de la collecte de logs (c’est-à-dire autres que les produits/SaaS du fournisseur de SIEM), y compris les technologies réseau, les points d’extrémité/serveurs, le cloud (IaaS ou SaaS) et les applications d’entreprise leaders sur le marché. Cela doit inclure des partenariats bidirectionnels et formellement reconnus avec au moins 10 grands fournisseurs de technologies de sécurité.
- Chiffre d’affaires des licences et de la maintenance cloud-natives/SaaS (à l’exclusion des services gérés) dépassant 50 000 000 USD pour les 12 mois précédant le 1er février 2022, ou avoir 100 clients de production distincts avec des contrats directs sur des plateformes cloud-natives ou SaaS à la fin de cette même période.

- Au cours des 12 mois précédant le 1er février 2022, avoir reçu 15 % du chiffre d'affaires cloud/SaaS de SIEM de la part d'acheteurs ayant un siège social hors de la région géographique du siège social du fournisseur, ou ayant au moins 20 clients de production, chacun ayant un siège social en dehors de la région géographique du siège social du fournisseur.
- Opérations de vente et de marketing (par le biais de campagnes imprimées/par e-mail, traductions en langue locale pour les supports de vente/marketing) promouvant les produits SIEM ciblant au moins deux régions géographiques à compter du 1er février 2022.

Les éléments suivants ont été exclus de la prise en compte :

- Capacités disponibles uniquement par le biais d'une relation de services gérés, c'est-à-dire la fonctionnalité SIEM disponible pour les clients uniquement lorsqu'ils souscrivent une offre de sécurité gérée d'un fournisseur, de détection et de réponse gérées, ou de SIEM géré, ou d'autres offres de services gérés. Par services gérés, nous entendons ceux dans lesquels le client engage le fournisseur pour établir, superviser, faire remonter et/ou répondre aux alertes, incidents et cas d'investigations.

Mentions honorables

- **DataDog** n'a pas été interrogé dans le cadre de ce processus Magic Quadrant, mais sa solution est considérée équivalente aux produits SIEM par les clients de Gartner en raison de son architecture cloud-native, de ses capacités de traitement des logs et de ses visualisations. DataDog exploite également une version freemium de son produit, y compris des fonctions de supervision de l'infrastructure. DataDog est une option pour les acheteurs qui se concentrent sur la collecte de logs et l'analyse manuelle.
- **Graylog** n'a pas satisfait aux exigences fonctionnelles pour figurer dans ce Magic Quadrant. Graylog est un autre fournisseur de SIEM qui a commencé par assurer la supervision de l'infrastructure et des applications, avant de proposer une prise en charge des scénarios d'utilisation des opérations de sécurité. La société propose désormais Graylog Security, qui comprend du contenu SIEM et UEBA pré-packagé, prêt à l'emploi, sous une seule licence.
- **Logsign** n'a pas satisfait aux exigences commerciales pour figurer dans ce Magic Quadrant. Logsign séduira les acheteurs connaissant Elasticsearch. Cette solution offre une combinaison de fonctionnalités SOAR et SIEM construites autour d'une interface utilisateur rationalisée avec des tableaux de bord personnalisables.
- **Google Chronicle** n'a pas été interrogé dans le cadre de ce Magic Quadrant. Chronicle présente un avantage natif évident pour les organisations ayant une présence Google Cloud importante et s'intègre à Google Security Command Center. Chronicle est capable d'ingérer des logs à grande échelle et offre des capacités de recherche rapides. Grâce à l'acquisition de Siemplify, Chronicle peut désormais être associé à une fonctionnalité SOAR.
- **Panther Labs** n'a pas satisfait aux exigences commerciales pour figurer dans ce Magic Quadrant. Elle offre une plateforme cloud-native de détection en tant que code comme alternative SIEM pour la détection des menaces axée sur le cloud, et peut prendre en charge les entrepôts de données AWS et Snowflake. Panther Labs offre également une architecture serverless et est entièrement gérée par son équipe d'assistance.

Critères d'évaluation

Capacité d'exécution

Produit ou service : ce critère évalue la capacité d'un fournisseur à fournir des fonctions de produit dans les domaines SIEM de base, comme la capacité à créer, modifier et maintenir des scénarios d'utilisation de détection des menaces, à fournir une gestion des cas et à soutenir les activités de réponse aux incidents, et à générer des rapports pour répondre aux besoins de l'entreprise, de la conformité et de l'audit.

Viabilité globale : ce critère comprend une évaluation de la traction client d'un fournisseur, du succès financier et pratique de son activité SIEM SaaS, et des indicateurs indiquant qu'il continuera à investir dans la technologie SIEM.

Exécution commerciale/tarification : ce critère évalue la réussite d'un fournisseur sur le marché du SIEM et ses capacités dans les activités de prévente. Les considérations comprennent la taille de son chiffre d'affaires SIEM et sa base installée pour son chiffre d'affaires SIEM cloud-natif/SaaS et sa base installée, la flexibilité des modèles de tarification, son support avant-vente, et la distribution et l'inclusivité de son canal de vente. Le niveau d'intérêt et les expériences examinées par les clients de Gartner sont également pris en compte.

Réactivité commerciale/Historique : Ce critère évalue les caractéristiques fournies et l'alignement sur la demande des clients pour les capacités de SIEM adjacentes et les méthodes de déploiement modernes, ainsi que les antécédents de livraison de fonctions nouvelles et différenciées en fonction de l'évolution des besoins du marché. Les considérations comprennent la prise en charge de la supervision multicloud, l'orientation commerciale cloud-native ou SaaS, et la prise en charge spécifique au secteur dans des domaines tels que l'OT.

Exécution marketing : Ce critère évalue les messages du marché SIEM d'un fournisseur à la lumière de la compréhension des besoins des clients par Gartner. Il identifie également les variations spécifiques identifiées par le fournisseur par secteur ou segment géographique.

Expérience client : ce critère évalue la fonction du produit et l'expérience du service dans les environnements de production. Sont incluses les fonctionnalités d'exploitation, d'administration et d'assistance aux fournisseurs. Ce critère évalue des domaines tels que l'assistance et la formation disponibles, la personnalisation des interfaces utilisateur et prend en compte les interactions avec les clients Gartner qui utilisent ou ont effectué des évaluations concurrentielles de l'offre SIEM d'un fournisseur.

Opérations : ce critère évalue les capacités de service, d'assistance et de vente d'un fournisseur. Il comprend une évaluation de ces capacités dans plusieurs zones géographiques.

Tableau 1 : Critères d'évaluation de la Capacité d'exécution

Critères d'évaluation	*Pondération*
Produit ou service	Élevée
Viabilité globale	Moyenne

Critères d'évaluation	*Pondération*
Exécution commerciale/tarification	Élevée
Réactivité/Perception commerciale	Élevée
Exécution marketing	Moyenne
Expérience client	Moyenne
Opérations	Moyenne

Source : Gartner (octobre 2022)

Exhaustivité de la vision

Compréhension du marché : ce critère évalue la capacité d'un fournisseur à comprendre les besoins émergents des acheteurs et comment communiquer efficacement les solutions. Les fournisseurs de SIEM qui présentent le plus haut degré de compréhension du marché peuvent identifier comment la technologie et les changements dans les méthodes de travail se traduiront par une mise à jour des exigences concernant les opérations de sécurité, tout en répondant aux besoins des entreprises en matière de rapports sur les risques commerciaux et le retour sur investissement.

Stratégie marketing : ce critère évalue la capacité d'un fournisseur à communiquer la valeur et la différenciation concurrentielle de son offre de SIEM.

Stratégie commerciale : ce critère évalue l'utilisation par un fournisseur des filiales de vente directe et indirecte, de marketing, de service et de communication pour étendre la portée et la profondeur de sa portée sur le marché.

Stratégie d'offre (produit) : ce critère évalue l'approche d'un fournisseur en matière de développement et de livraison de produits, en mettant l'accent sur la manière dont les fonctionnalités et les caractéristiques correspondent aux exigences actuelles. Les plans de développement au cours des 12 à 18 prochains mois sont également évalués. Le marché du SIEM est mature : il y a peu de différenciation entre la plupart des fournisseurs dans des domaines tels que la prise en charge des périphériques réseau communs, des périphériques de sécurité, des systèmes d'exploitation et des capacités d'administration consolidées. Nous attribuons des pondérations plus élevées à la couverture des sources d'événements émergentes, telles que l'IaaS et le SaaS, et au contexte environnemental.

Modèle commercial : malgré l'accent mis par les fournisseurs sur l'expansion de leurs capacités, nous continuons à valoriser la vitesse et la simplicité du déploiement et l'étendue du support de la plateforme. Les

utilisateurs, en particulier ceux dont les ressources informatiques et de sécurité sont limitées, apprécient toujours cet attribut plutôt que l'étendue de la couverture au-delà des scénarios d'utilisation de base. La nature déjà complexe des produits de SIEM tend à se renforcer à mesure que les fournisseurs étendent leurs capacités. Les fournisseurs capables de proposer des produits efficaces que les utilisateurs peuvent utiliser avec succès en tant que service, ou déployer, configurer et gérer avec des ressources limitées, seront les plus efficaces. Nous évaluons les options de déploiements cogérés ou hybrides de la technologie SIEM et des services d'assistance, car un nombre croissant de clients Gartner anticipent ou demandent des wrappers de services livrés par les fournisseurs (vendor-delivered service wrappers, VDSW) ou un support partenaire de fournisseur de services de sécurité pour superviser ou gérer leurs déploiements de technologie SIEM.

Stratégie verticale/sectorielle : ce critère évalue la stratégie d'un fournisseur pour prendre en charge les exigences SIEM spécifiques aux secteurs, comme les environnements de technologie opérationnelle (OT).

Innovation : ce critère évalue le développement et la mise à disposition par un fournisseur d'une technologie SIEM qui se distingue de celle de ses concurrents de manière à répondre de façon unique aux exigences les plus importantes des clients. Les capacités des produits et l'utilisation par les clients dans des domaines tels que la supervision de la couche applicative, la supervision orientée identité et l'investigation sur les incidents sont évaluées. Cela s'ajoute à d'autres capacités spécifiques au produit qui sont nécessaires et déployées par les clients. Une forte pondération est attribuée aux capacités nécessaires à la détection avancée des menaces et à la réponse aux incidents : supervision des utilisateurs, des données et des applications ; requêtes ad hoc ; visualisation ; orchestration et incorporation du contexte pour analyser les incidents ; et fonctionnalités de workflow/gestion des cas.

Stratégie géographique : ce critère tient compte du fait que, bien que les marchés d'Amérique du Nord et de la région EMEA génèrent le plus de revenus SIEM, l'Amérique latine et l'Asie/Pacifique sont des marchés en croissance pour le SIEM, et leur croissance est principalement motivée par la demande de gestion des menaces (et secondairement par les exigences de conformité). Notre évaluation globale des fournisseurs de ce Magic Quadrant comprend une évaluation de leurs stratégies de vente et d'assistance pour ces régions, ainsi que des fonctionnalités de produit pour répondre aux exigences de conformité locales et régionales en matière de résidence et de confidentialité des données.

Tableau 2 : Critères d'évaluation de l'exhaustivité de la vision

Critères d'évaluation	*Pondération*
Compréhension du marché	Élevée
Stratégie marketing	Moyenne
Stratégie commerciale	Moyenne
Stratégie d'offre (produit)	Élevée

Critères d'évaluation	*Pondération*
Modèle commercial	Faible
Stratégie verticale/industrielle	Moyenne
Innovation	Élevée
Stratégie géographique	Moyenne

Source : Gartner (octobre 2022)

Descriptions des Quadrants

Leaders

Les leaders fournissent des produits qui correspondent parfaitement aux exigences générales du marché. Ces fournisseurs ont été les plus performants dans la construction d'une base installée et d'une source de revenus sur le marché du SIEM. En plus de fournir une technologie qui correspond bien aux exigences actuelles des clients, les Leaders font preuve d'une vision et d'une exécution supérieures en matière d'exigences émergentes et anticipées. Ils ont généralement une part de marché relativement élevée et/ou une forte croissance du chiffre d'affaires, et reçoivent des commentaires positifs des clients sur leurs capacités SIEM et le service et l'assistance associés.

Challengers

Les Challengers ont plusieurs gammes de produits et/ou de services, au moins une base de clients SIEM de taille modeste, et des produits qui répondent à un sous-ensemble des exigences générales du marché. Les Challengers ont généralement de solides capacités d'exécution, comme en témoignent les ressources financières et une présence significative des ventes et de la marque. Cependant, les Challengers ne font pas preuve d'un ensemble complet de capacités SIEM ou manquent d'antécédents de réussite face à la concurrence avec les technologies SIEM comparables à ceux des Leaders.

Visionnaires

Les Visionnaires fournissent des produits qui correspondent parfaitement aux exigences générales du marché SIEM, mais qui ont moins de capacité d'exécution que les Leaders. Leur capacité d'exécution inférieure est généralement due à des scores inférieurs pour les caractéristiques et fonctions du produit, ou à une présence plus faible sur le marché SIEM que celle des Leaders. Cela est mesuré par la base installée, la taille ou la croissance du chiffre d'affaires, la taille globale de l'entreprise ou la viabilité générale (ou une combinaison de ces attributs).

Acteurs de niche

Les Acteurs de niche sont principalement des fournisseurs qui fournissent une technologie SIEM qui correspond bien à un scénario d'utilisation SIEM spécifique ou à un sous-ensemble des exigences fonctionnelles du marché SIEM. Les Acteurs de niche se concentrent sur un segment particulier de la clientèle (comme les organisations de taille moyenne, les prestataires de services ou une région ou un secteur spécifique) ou peuvent fournir un ensemble limité de capacités de SIEM. En outre, les Acteurs de niche peuvent avoir une petite base installée ou être limités, selon les critères de Gartner, par d'autres facteurs. Ces facteurs peuvent inclure des investissements ou des capacités limités, une empreinte géographique limitée, ou d'autres obstacles à la mise à disposition d'un large éventail de capacités aux organisations maintenant et pendant une période de planification de 12 mois. L'inclusion dans ce quadrant ne reflète pas négativement la valeur d'un fournisseur pour des marchés ou des scénarios d'utilisation étroitement ciblés.

Contexte

Le marché du SIEM continue d'ajouter plus de fonctionnalités et de stratégies d'architecture de changement pour répondre aux demandes des clients. Ce Magic Quadrant met l'accent sur la disponibilité de l'architecture SaaS globale et sur les fonctionnalités de plateforme multifacettes telles que SOAR, UEBA, TIP, la création analytique en libre-service, la création continue de contenu sur les menaces et les fonctionnalités de gestion des incidents. Les organisations qui continuent à rechercher des architectures auto-déployées et gérées trouveront de plus en plus leurs options limitées à mesure que de plus en plus de fournisseurs de SIEM passeront à des offres d'architecture SaaS prédominantes ou exclusives.

Les lecteurs devraient utiliser cette étude du Magic Quadrant comme l'une des nombreuses ressources pour faciliter leur décision d'achat, et non comme source unique de vérité. Les lecteurs ne doivent pas déduire qu'un fournisseur dans le quadrant Leaders est par défaut le meilleur choix pour son scénario d'utilisation ou environnement particulier. Évaluez les fournisseurs par rapport à vos besoins commerciaux et de sécurité individuels, et non par rapport à leur position dans le quadrant.

Cette étude évalue les fournisseurs en fonction de leurs solutions telles qu'elles ont été proposées en 2021 jusqu'au 1er février 2022, afin d'évaluer l'efficacité de leurs plans d'action de produits SIEM. Le marché du SIEM évolue en permanence, ce qui signifie que cette étude est une évaluation ponctuelle. À ce titre, les lecteurs doivent tirer parti de l'étude Capacités critiques associées liées à la gestion des informations et des événements de sécurité, qui peut tenir compte de mises à jour hors cycle tout au long de l'année, lorsque les fournisseurs apportent des changements significatifs qui justifient une mise à jour de la notation de leurs Capacités critiques.

Aperçu du marché

Le marché du SIEM est passé de 3,41 milliards de dollars en 2020 à 4,10 milliards de dollars en 2021 (voir Market Share : All Software Markets, Worldwide, 2021), un taux de croissance annuel de 20 % par rapport à une baisse de 3,9 % l'année précédente. Les principaux moteurs d'un achat de SIEM sont la détection des menaces, la réponse, la gestion de l'exposition et la conformité. Les acheteurs recherchent un écosystème SIEM doté de capacités étendues et approfondies pour satisfaire plusieurs scénarios d'utilisation de sécurité et d'entreprise avec des capacités pour prendre en charge un environnement diversifié.

Le marché du SIEM évolue à un rythme rapide et continue d'être extrêmement compétitif. La réalité de ce qu'était le SIEM il y a seulement cinq ans commence à se détacher de ce que le SIEM est et fournit aujourd'hui.

Le SIEM prend désormais largement en charge les capacités de gestion de l'exposition en tirant parti des points de données tels que l'état de configuration des actifs cloud, le profilage des risques entre les utilisateurs et les entités, l'inventaire des actifs et la notation de la criticité, dans le but de fournir une posture de risque en temps réel. Cette combinaison de scénarios d'utilisation aide les responsables de la sécurité et de la gestion des risques (security and risk management, SRM) à élaborer une analyse de rentabilisation convaincante pour les achats en fonction des indicateurs de résultats obtenus (voir Tool : Catalog of Business-Aligned Outcome-Driven Metrics for Risk and Security), qui peut répondre aux questions de l'entreprise sur la valeur qu'un SIEM apportera plutôt que de se concentrer sur le coût.

Le marché du SIEM s'est tourné vers une solution de sécurité riche en fonctionnalités pour offrir aux clients de nombreuses options pour répondre à leurs besoins en matière de sécurité, comme :

Détection des menaces :

- Analyses en temps réel
- Analyse des lots
- Algorithmes de science des données
- Analyses basées sur les utilisateurs et les entités

Réponse :

- SOAR
- Gestion des incidents
- Collaboration

Gestion de l'exposition :

- Détails des actifs (criticité, groupement, emplacement, état du correctif, etc.)
- Détails de l'utilisateur (criticité, groupement de pairs, unité commerciale, rôle, historique des incidents, etc.)
- Posture de configuration (configuration des actifs cloud, paramètres GPO, etc.)
- Visibilité multicloud et compréhension unifiée de l'exposition
- Alignement du cadre de détection des menaces

Conformité :

- Rapports
- Exigences de supervision continue
- Audits

- Système d'enregistrement de sécurité

L'architecture de déploiement la plus importante est passée d'une architecture hébergée et gérée par le client, à une architecture cloud native (SaaS) ou fournie par le cloud (hébergée) pour tirer parti de déploiements plus faciles, d'une évolutivité et d'une flexibilité accrues. Les options SaaS réduisent les exigences des acheteurs en matière de gestion et de maintenance d'un déploiement SIEM, ce qui leur permet de se concentrer sur les résultats de sécurité, plutôt que sur l'application de correctifs et la mise à niveau des versions matérielles et logicielles SIEM. Cette transition vers le SaaS a incité les petites et moyennes entreprises à investir dans le SIEM pour avoir la garde de leurs données de sécurité, et la croissance actuelle du marché le confirme. En retour, nous avons observé une augmentation des services SIEM cogérés pour assurer la supervision et l'optimisation à plein temps des solutions SIEM des clients. Il existe des marchés où les architectures sur site/hébergées restent une exigence (pour l'instant) et les fournisseurs de SIEM doivent continuer à étendre l'assistance dans les centres de données des fournisseurs de cloud régionaux. Les lois sur la souveraineté des données et la confidentialité continueront d'avoir un impact sur la résidence et l'accès aux données, que les fournisseurs de SIEM peuvent traiter en déployant leurs solutions au niveau régional, et limiteront la résidence des données en fonction des exigences de l'acheteur.

Le marché du SIEM continuera d'évoluer et verra une concurrence accrue avec de nouvelles solutions qui sont arrivées sur le marché. La détection et la réponse étendues (Extended detection and response, XDR) ciblent les organisations dont la posture des opérations de sécurité est moins avancée, ou qui n'ont pas la capacité d'exécuter une solution SIEM complexe. Ces acheteurs sont enclins à acheter des wrappers de services livrés par les fournisseurs (vendor delivered service wrappers, VDSW) auprès de leur fournisseur de technologie de choix pour exécuter la solution de sécurité qu'ils ont achetée en raison du manque de ressources.

Les fournisseurs de SIEM ont déjà commencé à investir dans (ou à acquérir) des solutions de collecte de télémétrie pour fournir un écosystème préconstruit de technologies de sécurité aux acheteurs qui recherchent une solution de sécurité encapsulée. Une solution qui offre des fonctionnalités de détection des menaces, de conservation des logs de sécurité, de reporting de conformité, d'analytique comportementale, d'automatisation, d'investigation et d'actions d'intervention. Les solutions de sécurité SIEM, UEBA, SOAR, TIP, EDR, NDR et cloud dans une offre groupée sont déjà sur le marché, et cette tendance devrait continuer à croître. Cela s'aligne sur le concept du maillage de cybersécurité et d'une architecture de sécurité modulaire. Cependant, il est irréaliste de s'attendre à ce que chaque organisation souhaite qu'un seul fournisseur fournisse l'ensemble de sa pile de sécurité, ce qui permettra de continuer à mettre en concurrence les fournisseurs à l'avenir.

Définitions des critères d'évaluation

Capacité d'exécution

Produit/Service : les biens et services de base offerts par le fournisseur pour le marché défini. Cela inclut les capacités actuelles des produits/services, la qualité, les ensembles de fonctionnalités, les compétences, etc., qu'ils soient proposés nativement ou par le biais d'accords/partenariats OEM, tels que définis dans la définition du marché et détaillés dans les critères secondaires.

Viabilité globale : la viabilité comprend une évaluation de la santé financière globale de l'entreprise, de la réussite financière et concrète de l'unité commerciale, et de la probabilité que l'unité commerciale

individuelle continue à investir dans le produit, à le commercialiser et à faire progresser la technologie au sein du portefeuille de produits de l'entreprise.

Exécution commerciale/tarification : les capacités du fournisseur dans toutes les activités d'avant-vente et la structure qui les sous-tend. Cela comprend la gestion des transactions, la tarification et la négociation, l'assistance avant-vente et l'efficacité globale du canal de vente.

Réactivité commerciale/Historique : la capacité à réagir, à changer de direction, à être flexible et à semer la concurrence lorsque les opportunités se développent, que les concurrents agissent, que les besoins des clients évoluent et que la dynamique du marché change. Ce critère tient également compte de la réactivité du fournisseur par le passé.

Exécution marketing : La clarté, la qualité, la créativité et l'efficacité des programmes conçus pour transmettre le message de l'organisation afin d'influencer le marché, de promouvoir la marque et l'entreprise, d'accroître la notoriété des produits, et de susciter une identification positive du produit/de la marque et de l'organisation dans l'esprit des acheteurs. Cette « notoriété » peut être motivée par la combinaison de publicité, d'initiatives promotionnelles, de leadership éclairé, de bouche-à-oreille et d'activités commerciales.

Expérience client : les relations, produits et services/programmes qui favorisent le succès des clients avec les produits évalués. Cela inclut plus précisément la manière dont l'assistance technique ou la gestion de compte est fournie aux clients. Cela peut également inclure des outils auxiliaires, des programmes d'assistance client (et leur qualité), la disponibilité de groupes d'utilisateurs, des contrats de niveau de service, etc.

Opérations : La capacité de l'organisation à atteindre ses objectifs et à respecter ses engagements. Les facteurs comprennent la qualité de la structure organisationnelle, dont notamment les compétences, expériences, programmes, systèmes et autres moyens qui permettent à l'organisation de fonctionner de manière efficace et efficiente de façon continue.

Exhaustivité de la vision

Compréhension du marché : la capacité du fournisseur à comprendre les désirs et les besoins des acheteurs et à les traduire en produits et services. Les fournisseurs qui affichent le plus haut degré de vision écoutent et comprennent les désirs et les besoins des acheteurs, et peuvent les façonner ou les améliorer en y ajoutant leur propre vision.

Stratégie marketing : ensemble de messages clairs et différenciés qui sont communiqués avec cohérence dans toute l'organisation et à l'extérieur par le biais d'un site web, de messages publicitaires, de programmes destinés aux clients et de déclarations de positionnement.

Stratégie commerciale : la stratégie de vente de produits qui utilise le réseau approprié de sociétés affiliées de vente directe et indirecte, de marketing, de service et de communication. Celles-ci étendent le périmètre et la profondeur de la portée commerciale, des compétences, de l'expertise, des technologies, des services et de la clientèle.

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

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

Stratégie verticale/sectorielle : la stratégie du fournisseur visant à allouer les ressources, les compétences et les offres de manière à répondre aux besoins spécifiques des segments de marché individuels, y compris les marchés verticaux.

Innovation : les dispositions directes, connexes, complémentaires et synergiques des ressources, de l'expertise ou du capital à des fins d'investissement, de consolidation, de défense ou de prévention.

Stratégie géographique : stratégie du fournisseur pour allouer ses ressources, ses compétences et ses produits en fonction des besoins précis de régions géographiques en dehors du territoire initial, que ce soit de façon directe ou par le biais de partenaires, de canaux et de filiales implantés dans ces autres territoires et marchés.