Part de marché

Part de marché mondial de la gestion des événements et des informations de sécurité en 2018 : selon la taille des entreprises – la volonté de répondre à tous les besoins des clients

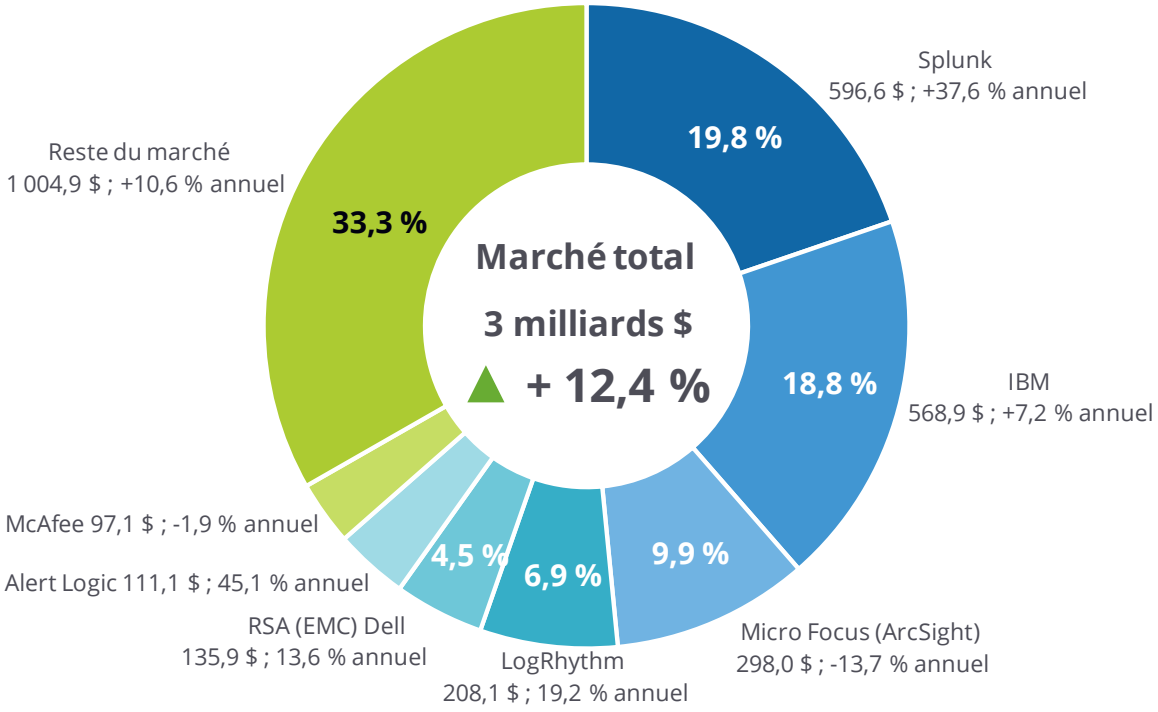
Christopher Kissel Frank Dickson

CET EXTRAIT DU DOCUMENT D'IDC SUR LES PARTS DE MARCHÉ CONCERNE SPLUNK

FIGURE D'IDC PRÉSENTANT LES PARTS DE MARCHÉ

FIGURE 1

Vue générale des parts de marché mondial de la gestion des événements et des informations de sécurité en 2018 :



Remarque : Parts de marché (%), chiffre d'affaires (M $) et croissance (%) en 2018

Source : IDC, 2019

Juin 2019, IDC N° US45161819e

DANS CET EXTRAIT

Cet extrait provient directement du document *Worldwide Security Information and Event Management Market Shares, 2018: By Size of Business – The Attempt to Serve All Client Needs* (Part de marché mondial de la gestion des événements et des informations de sécurité en 2018 : selon la taille des entreprises – la volonté de répondre à tous les besoins des clients) (Doc. N° US45161819). Les sections mentionnées ci-dessous figurent en partie ou en totalité dans cet extrait : Résumé ; Parts de marché ; Les acteurs qui ont compté cette année ; Contexte du marché ; Annexe ; En savoir plus.

RÉSUMÉ

IDC estime que le chiffre d'affaires des fournisseurs de produits et de services de gestion des événements et des informations de sécurité (SIEM) a augmenté de 12,4 % en 2018 pour atteindre une valeur d'un peu plus de 3 milliards de dollars. Le SIEM constitue toujours un outil de base et essentiel pour la cybersécurité. De manière générale, le besoin d'une solution SIEM est de plus en plus important au fur et à mesure que la taille de l'entreprise augmente. Traditionnellement, les plateformes SIEM sont utilisées pour générer des rapports de conformité – une fonction importante à l'heure actuelle. Elles sont également utilisées pour le stockage et l'indexation de paquets à des fins d'investigation ; on espère aujourd'hui pouvoir assurer le suivi des alertes faisant l'objet d'une investigation pour déterminer les délais de détection des menaces dans l'environnement d'un réseau. Chaque session de navigation Internet, e-mail, transaction interne de serveur et routeur, ou encore requête Active Directory, génère un enregistrement. En théorie, en disposant de suffisamment de temps et des bonnes compétences, les journaux pourraient être reconstruits afin de savoir à quel moment l'adversaire s'est introduit dans le réseau, quelles propriétés numériques ont été exfiltrées et quel chemin d'extraction a été utilisé. On peut raisonnablement affirmer que la collecte intelligente de métadonnées offre un moyen de cyberdéfense efficace et rentable, mais une capture de paquets complets (PCAP) est nécessaire pour pouvoir reconstruire les chronologies d'événements avec les artefacts originaux. En s'appuyant également sur des moyens d'expertise légale, le SIEM représente le dernier espoir de pouvoir attraper l'adversaire.

Naturellement, le scénario du « dernier espoir » reste pessimiste même dans le meilleur des cas. À partir de 2015, les fournisseurs de solutions SIEM ont fourni de sérieux efforts pour réinventer leurs produits qualifiés de SIEM de nouvelle génération ou SIEM 2.0. Le SIEM de nouvelle génération reposait sur l'idée que le SIEM pourrait constituer la meilleure plateforme de détection des menaces en temps réel. Cette affirmation n'était pas totalement infondée, et elle ne l'est toujours pas. Vers 2015, le principal problème en matière de cybersécurité résidait dans le fait qu'elle se basait sur les signatures de malware et impliquait une réponse après coup. Certes, des sources de renseignement sur les menaces restent disponibles, mais les pare-feux, les antivirus et la protection des terminaux agissent généralement lorsque les signatures de malware connues sont interfacées avec des solutions technologiques. L'avenir du SIEM reposait sur l'introduction de l'analyse du comportement des utilisateurs (UBA pour User Behavioral Analytics) supposée constituer un dernier rempart et fournir un moyen de suivre les menaces *zero day* de type « low and slow », c'est-à-dire à diffusion lente et a priori insignifiantes.

Deux indicateurs principaux permettent d'évaluer l'efficacité d'un centre des opérations de sécurité (SOC) : le délai moyen de détection (MTTD) et le délai moyen de réponse (MTTR). Le SIEM étant une technologie qui repose sur les journaux, elle peut donc améliorer ces deux indicateurs. En 2019, l'UBA constitue un complément important des dispositifs globaux de cybersécurité. Il s'agit d'une solution

discrète offrant un ensemble de fonctionnalités essentielles utilisées avec de multiples solutions technologiques telles que la détection et les réponses au niveau des terminaux, les analyses des menaces et le SIEM. L'UBA doit être appréhendée comme un ensemble analytique établissant des liens individuels pour chaque entité au sein d'un réseau. L'application de l'UBA permet d'établir une référence statistique qui ne servira pas uniquement de base pour les comportements déviants, mais pourra également servir d'« image de référence » de ce qu'est un appareil et de ce qu'il doit faire. Dans le cadre du SIEM, l'UBA peut affiner et indexer (de manière optimale) l'état des machines ou des identités sur plusieurs sources de journaux, ce qui permet de résoudre le problème de MTTD.

Le SIEM devra ensuite mettre l'accent sur l'amélioration du MTTR. Si le SIEM ingère de façon bidirectionnelle des données de journaux et de flux depuis de nombreuses sources de journaux, il va de soi que la même connectivité peut être utilisée pour renforcer la surface de la cybersécurité. Concernant l'orchestration, avec les bonnes API ou la bonne plateforme d'orchestration de la sécurité, le SIEM peut envoyer les signatures de malware associées à des alertes basées sur des règles, des rôles, des risques, des anomalies d'UBA ou des alertes précises en corrélant ces événements aux pare-feux, terminaux, systèmes de détection des intrusions (IDS), systèmes de prévention des intrusions (IPS), etc. Cela est possible avec ou sans intervention manuelle. Concernant l'automatisation, les utilisations possibles de l'automatisation découlant du SIEM sont innombrables, y compris l'écriture et l'importation de nouvelles règles pour un pare-feu de nouvelle génération, l'envoi de fichiers vers une sandbox, la mise en quarantaine de machines ou le déclenchement d'un flux de travail pour les analystes SOC.

Il faut néanmoins reconnaître qu'il reste encore beaucoup à découvrir ici. Les principes de la gestion des journaux et du SIEM en mutation constante datent d'environ 25 ans. En matière de technologie, les logiciels ou les produits qui durent aussi longtemps sont rares, et le fait qu'une technologie connaisse toujours une croissance à deux chiffres d'une année sur l'autre peut surprendre. Cependant, la longue explication fournie précédemment concernant l'utilisation adéquate du SIEM pose également les fondations de ce à quoi ressemble la cybertechnologie dans un cadre concurrentiel. Tout au long de ce document, nous préciserons en quoi les plateformes de SIEM se différencient les unes des autres, et nous expliquerons partiellement pourquoi le SIEM, envisagé en tant qu'ensemble technologique, suscite des préoccupations face aux autres approches employées en matière de cybersécurité.

Cette étude d'IDC fournit des données sur les parts de marché mondial de la gestion des événements et des informations de sécurité selon la taille des entreprises.

Selon Chris Kissel, directeur de recherche chez IDC, produits de cybersécurité dans le monde, « Actuellement, le SIEM joue un rôle central et crucial dans le dispositif global de cybersécurité des entreprises ». « Cependant, les fournisseurs de solutions de SIEM devront répondre aux besoins émergents en matière d'Internet des Objets (IoT) et seront confrontés à l'hétérogénéité des réseaux. Et bien que le SIEM offre une visibilité unique et facilite l'orchestration avec d'autres plateformes de cybersécurité, les fournisseurs de solutions de SIEM devront se mesurer aux fournisseurs de plateformes d'analyse de sécurité, de détection et de réponse au niveau des terminaux (EDR) et aux solutions open source pour conserver leurs parts de marché ».

CONSEILS POUR LES FOURNISSEURS DE SOLUTIONS TECHNOLOGIQUES

Dans ce document, nous utilisons le terme SIEM pour désigner globalement les plateformes qui ingèrent différents journaux et flux, disposent de tableaux de bord spécifiquement utilisés pour

enquêter sur les menaces, commencent à y remédier et sont capables de produire des rapports de conformité. Dans les faits, les différentes formes de plateformes peuvent avoir une influence sur la proposition de valeur qui leur est associée. Les solutions SIEM en tant que service (basées sur le cloud), les environnements hétérogènes (environnements mixtes associant le cloud public, le cloud privé et des infrastructures sur site), et les solutions sur site avec archivage des fichiers PCPA sont fondamentalement différentes. Bien que les fournisseurs de solutions de SIEM optent pour des approches sensiblement différentes selon la taille de l'entreprise cliente, les qualités (détaillées ci-après) que doivent présenter les fournisseurs pour conquérir de nouveaux clients et conserver les clients existants sont universelles. Elles doivent répondre aux propositions de valeur suivantes et les présenter à leurs acheteurs potentiels :

- **Présenter préalablement les conditions tarifaires.** Nous sommes conscients qu'il ne s'agit pas d'une demande occasionnelle. Deux parties agissant de bonne foi peuvent ne pas appréhender correctement ce qui se trouve dans un réseau donné jusqu'à ce qu'une appliance soit complètement installée ou un service soit lancé. Les clients n'ont pas besoin de savoir si une licence est basée sur un nombre d'événements ou de messages par seconde (cas de figure le plus courant), sur des appliances ou des collecteurs/transmetteurs, ou une durée définie. Le fournisseur doit également expliquer ce qu'il se passera si le client atteint ses limites de capacité et comment il prendra en charge les périodes d'utilisation intense (par exemple, pour les commerçants en ligne pendant la période de Noël).
- **Déterminer les besoins en capacité de stockage.** Au cours de certaines instances sur site, l'utilisateur collectera des paquets complets et les stockera sur site. Cependant, IDC estime qu'il incombe au fournisseur SIEM de proposer des solutions d'organisation du trafic, telles que Gigamon et Ixia, lorsqu'une collecte de métadonnées est appropriée ou lorsqu'un stockage en ligne suffit.
- **Prévoir comment une solution de SIEM fonctionnera dans l'environnement du prospect.** Les principales solutions de SIEM, telles que celles de Splunk, d'IBM, de Micro Focus, de LogRythm, de RSA et de McAfee, seront largement intégrées aux principales solutions de pare-feu, de protection des terminaux, d'EDR et d'IDS/IPS. Bien que le coût d'une solution tierce ne sera probablement pas affecté par une licence SIEM, qu'il existe ou non une appliance en tant que module d'intégration à part entière ou que des API soient développées selon la spécification OpenAPI, du temps et de l'argent seront nécessaires pour configurer les appareils.
- **S'interroger sur les capacités de la solution SIEM dans les environnements en développement.** Traditionnellement, le SIEM n'est pas un outil important dans les environnements DevOps, car les conteneurs sont déployés et retirés dans le cadre d'applications spécifiques et ponctuelles. Toutefois, les applications spécifiques risquent de devenir fréquentes au fur et à mesure que la promesse de l'IoT se concrétise. Concernant l'IoT, les fournisseurs doivent articuler leur stratégie afin de pouvoir assurer un suivi des appareils IoT du point de vue des identités ou de la sécurité au sein de leur SIEM.
- **Tenir compte des environnements de cloud public.** Une grande partie des tâches requises pour une collecte dans le cloud public est prise en charge par les fournisseurs de cloud public eux-mêmes (en matière de certification des plateformes). Le VTAP de Microsoft supporte tous les produits de sécurité pour les terminaux. La majorité des solutions de SIEM offre des moyens de collecter les flux issus des applications SaaS répandues telles qu'Office 365 et Salesforce.
- **Reconnaître que les coûts indirects ont de l'importance.** Un certain nombre de facteurs peuvent faire grimper rapidement le coût total de possession d'une solution de SIEM. Comme

nous l'avons mentionné, la qualité des API en fait partie ; le fournisseur doit être transparent concernant ses possibilités en matière d'assistance à l'écriture de scripts ou, au moins, de fourniture de bibliothèques. Les analystes de sécurité ne se valent pas tous. Bien que la maintenance et le support soient généralement facturés en supplément de la solution logicielle (généralement pour un montant égal à 20 % du coût du logiciel ou du service), les heures d'assistance technique doivent être précisées préalablement.

- **Offrir des capacités de détection des menaces, mais pas seulement.** Les entreprises qui proposent des solutions concurrentes aux solutions SIEM s'appuient sur les analyses pour la veille économique. Elles prennent facilement en charge les scénarios basés sur des hypothèses. Outre la suppression complète d'une violation, la solution SIEM peut également proposer des fonctionnalités de simulation d'attaque ou doit être en mesure d'émettre des hypothèses sur les conséquences que pourraient avoir une menace répandue sur le réseau (WanaCry et Petya sont des exemples récents de ce type de menaces). Diverses plateformes et certaines solutions SIEM sont capables d'utiliser des analyses du trafic réseau comme indicateurs de compromission (IOC), mais même si un goulot d'étranglement dans le réseau ne constitue pas un problème de sécurité, il ne coûte rien d'en informer l'équipe informatique de toute façon.
- **S'interroger sur les possibilités de migration vers des solutions SaaS.** Les solutions de suivi/détection/réponse (MDR) font partie des cyber-technologies émergentes. Les entreprises œuvrant dans ce domaine, telles qu'ArcticWolf et eSentire, collectent vos journaux, offrent un stockage illimité et proposent un SLA pour les rapports et les réponses aux alertes. Il existe un créneau entre les solutions traditionnelles de SIEM les solutions MDR pour les entreprises souhaitant apporter leurs propres réponses aux menaces et aux contraintes de stockage, mais qui veulent que le fournisseur de solutions SIEM prenne en charge les alertes et l'architecture du dispositif de cybersécurité.
- **Reconnaître ses responsabilités.** Même pour les fournisseurs de solutions SIEM, il existe un risque de perte des clients. Les clients sont de plus en plus contrariés par la perspective d'être verrouillés à un fournisseur. Bien qu'il semble que les fournisseurs de solutions SIEM puissent espérer rester discrets sur ce qu'il se passera au terme d'un contrat, à long terme, une discussion réfléchie sur le sort des fichiers chiffrés, les clés d'infrastructure de clés publiques (PKI), les identités et les paquets stockés permettra dans un premier temps de convaincre les clients et de faciliter ensuite les renouvellements de contrat.

PARTS DE MARCHÉ

Le Tableau 1 fournit des données sur les parts de marché détenues par 22 fournisseurs sur la base du chiffre d'affaires total enregistré en 2017 et en 2018, les évolutions constatées d'une année sur l'autre et la répartition du chiffre d'affaires selon le type d'entreprises – 1 à 999 employés, 1 000 à 2 499 employés, 2 500 à 9 999 employés et plus de 10 000 employés. Ces chiffres représentent la taille des entreprises acheteuses et non celle des centrales d'achat.

La Figure 2 illustre l'environnement concurrentiel dans lequel évoluent les cinq principaux fournisseurs sur le segment des entreprises de plus de 10 000 employés, ainsi que certaines des offres les plus évoluées des fournisseurs. Splunk, LogRhythm et Alert Logic sont les principaux acteurs ayant généré le chiffre d'affaires lié au SIEM. Mais il est difficile de savoir dans quelle mesure les tendances actuelles sont la conséquence d'actions marketing ou des possibilités d'utilisation offertes.

TABLEAU 1

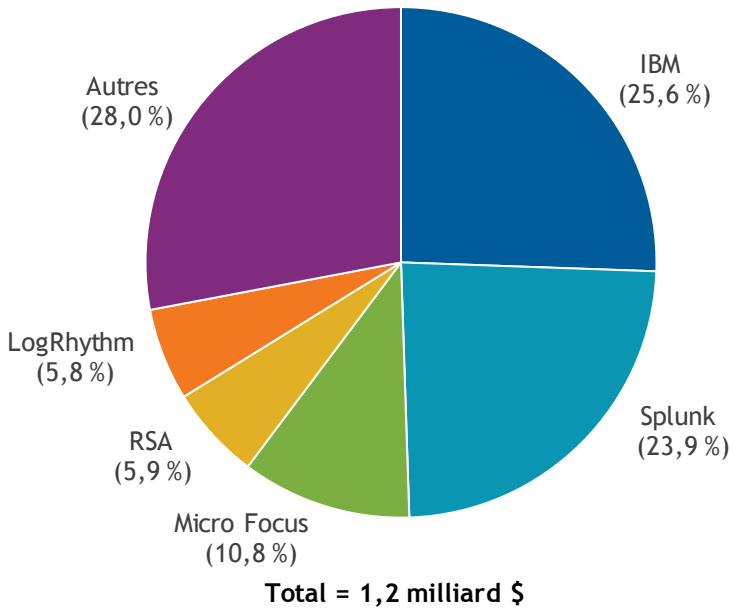
Chiffre d'affaires mondial tiré des ventes de solutions SIEM par fournisseur et taille d'entreprises en 2017 et 2018

	Chiffre d'affaires (M $)			Chiffre d'affaires selon les tailles d'entreprise évaluées en nombre d'employés (M $)			
Entreprise	2017	2018	Croissance de 2017 à 2018 (%)	1 à 999 employés	1 000 à 2 499 employés	2 500 à 9 999 employés	Plus de 10 000 employés
Splunk	433,5	596,6	37,6	13,8	63,8	220,7	298,2
IBM	530,7	568,9	7,2	5,7	45,5	199,1	318,6
Micro Focus (ArcSight)	345,1	298,0	- 13,7	3	8,9	152	134,1
LogRhythm	174,6	208,1	19,2	15,6	54,6	65	72,8
RSA (EMC) Dell	119,6	135,9	13,6	4,1	17,7	40,1	74
Autres	1 084,4	1 213	11,9	128,4	290	446,1	348,7
Total	2 687,9	3 020,5	12,4	170,6	480,5	1 123	1 246,4

Source : IDC, 2019

FIGURE 2

Répartition du chiffre d'affaires mondial tiré des ventes de solutions SIEM par fournisseur sur le segment des entreprises de plus de 10 000 employés en 2018



Source : IDC, 2019

L'environnement des SOC des entreprises se différencie par les budgets dont ces SOC disposent et les compétences de leurs analystes (constat qui n'a pas pour objet de minimiser les compétences des analystes des petites entreprises). Cependant, les entreprises ont un budget suffisant pour créer des postes d' « expert SIEM » et enrichissent régulièrement leur vivier de talents en puisant dans les ressources des plus petites entreprises. Cela signifie que ces SOC auront probablement plus d'outils à intégrer ; nous connaissons des SOC disposant de plus de 100 outils.

La connaissance des outils et leurs modalités d'utilisation sont des facteurs importants dans un SOC d'entreprise. L'orchestration et l'automatisation sont bien évidemment des considérations plus importantes pour les entreprises disposant d'une trentaine d'outils que pour les grandes entreprises ou les SOC de taille moyenne utilisant 10 à 15 outils différents. IDC estime qu'IBM Resilient a aidé IBM à développer progressivement ses activités, et l'intégration étroite de Splunk avec Phantom a joué un rôle clé dans l'expansion rapide de Splunk sur le marché SIEM.

Cependant, il existe une problématique inhérente au SIEM pour les entreprises. Bien que la prise en charge d'une multitude de sources de journaux puisse contribuer à découvrir des vecteurs de menace que les signatures de malware utilisées isolément ne permettront pas de mettre à jour, l'ingestion et le stockage des données impliquent des coûts. Splunk est l'entreprise à laquelle il est le plus souvent fait référence en raison du modèle de consommation qu'elle propose. IDC pense que les entreprises auront généralement tendance à s'éloigner des solutions SIEM basées sur des modèles à l'usage, mais rien ne prouve que Splunk en soit actuellement affectée.

Exabeam se révèle être un digne concurrent sur le secteur des solutions SIEM. Cette entreprise a forgé sa réputation dans le domaine de l'UBA, mais elle vend actuellement des licences pour des solutions de compléments et de remplacement SIEM. L'offre SIEM d'Exabeam est proposée sous la forme d'une solution SaaS et sur site. Exabeam peut ainsi modifier dynamiquement sa plateforme depuis laquelle une nouvelle protection peut être communiquée à de nombreuses autres plateformes. Surtout, Exabeam facture ses services en fonction du nombre d'utilisateurs et non en fonction des sources de journaux ou de l'usage.

Dans sa version actuelle, Exabeam ingère plus de 200 sources de journaux. Exabeam s'appuie sur une hiérarchie d'indexation bien définie utilisant 2 500 analyseurs. « Analyser » les données permet d'avoir une visibilité en temps réel au fur et à mesure que la source de journaux est assemblée et analysée sur la plateforme Smart Timelines. Celle-ci utilise l'environnement de développement MITRE ATT&CK, ce qui signifie que de nombreuses étapes d'investigation sont préassemblées dans la solution SIEM.

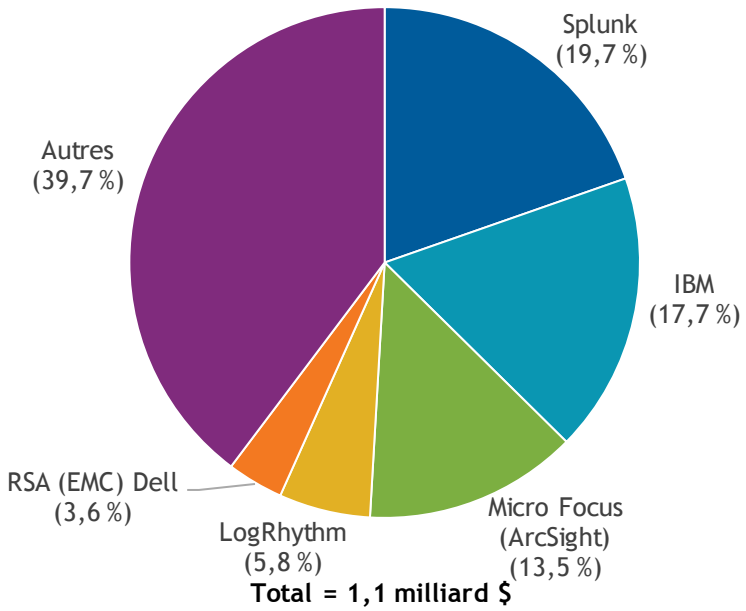
Pour des raisons évidentes, les solutions SIEM d'entreprise font l'objet de nombreuses critiques. Finalement, parmi tout ce qu'un fournisseur d'outils de sécurité peut apporter, le plus important concerne le MTTD et le MTTR. Lorsque les dépenses entrent moins en ligne de compte, la solution SIEM est en concurrence avec d'autres solutions SIEM de fournisseurs d'analyse des menaces de sécurité tels que DarkTrace et Anomali et avec les solutions des fournisseurs de services gérés de sécurité (MSSP). Par rapport aux solutions d'EDR, le SIEM sera davantage vu comme une solution complémentaire plutôt que comme une solution concurrente.

En termes de plateforme, les fournisseurs de solutions SIEM doivent se montrer compétitifs pour chaque composante individuelle que l'on retrouve dans un SIEM et disposer de capacités sensiblement supérieures à celles que l'on trouve sur des plateformes ouvertes pour séduire les entreprises de 2 500 à 9 999 employés (voir Figure 3). Citons quelques exemples pratiques de solutions concurrentes :

- **Services gérés et professionnels.** En général, les MSSP sont trop chers et les grandes entreprises peuvent ne pas souhaiter externaliser leur informatique ; cela dit, les MSSP restent dans la course.
- **MDR.** Les fournisseurs de solutions MDR proposent une gestion des alertes et des SLA portant sur les alertes. Il s'agit d'une alternative séduisante ou du moins, d'une solution complémentaire viable pour les SOC.
- **Architectures de SOC hybrides.** Pour faire des économies, un SOC pourra utiliser des éléments d'une pile open source ELK (Elasticsearch, Logstash, et Kibana). On peut imaginer qu'un SOC utilise le cloud public ou un périphérique de stockage en réseau (NAS) pour le stockage, Elasticsearch et Bro pour la détection des menaces en contournant totalement le SIEM.
- **Plateformes de gestion des données dans le domaine de la sécurité.** Cloudera propose un cas d'usage efficace. Les développeurs peuvent utiliser RedEx, Python ou Scala pour les traitements à la demande. Les données sont stockées de façon à ce que les experts en mégadonnées puissent tester des hypothèses sur la plateforme sans perturber le flux de travail.
- **Plateformes de détection des menaces.** La capacité de visualiser les menaces est toujours aussi importante dans ces SOC. Les entreprises de cette taille ne sont pas contre l'utilisation d'une solution SIEM pour la collecte des journaux, mais elles utilisent une plateforme d'analyse de sécurité, telles que Vectra ou Darktrace, pour la visualisation ou l'UBA.

FIGURE 3

Répartition du chiffre d'affaires mondial tiré des ventes de solutions SIEM par fournisseur sur le segment des entreprises de 2 500 à 9 999 employés en 2018



Source : IDC, 2019

En se basant uniquement sur l'importance de son chiffre d'affaires, IDC estime que Splunk est toujours leader sur le segment des entreprises de 1 000 à 2 499 employés (voir Figure 4). LogRythm se pose en concurrent, tandis qu'Alert Logic et AlienVault (AT&T désormais) sont sur le point de gagner des parts de marché en 2019.

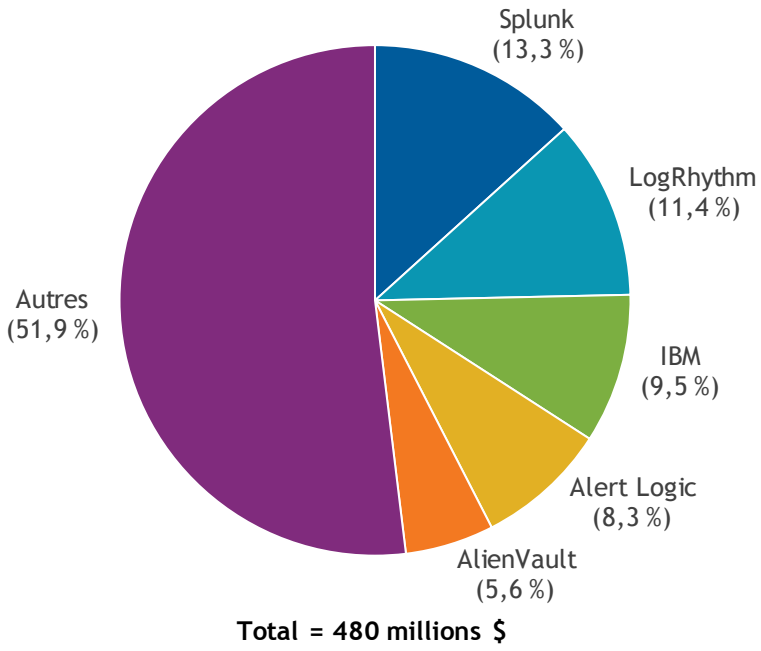
Les facteurs concurrentiels sont en grande partie les mêmes pour les entreprises de 2 499 employées et celles de 9 999 employés, à deux exceptions notables près. Pour les entreprises de taille moyenne, les hôtes cloud constituent des éléments potentiellement perturbateurs pour le SIEM. Par exemple, AWS offre un stockage de deux événements par seconde (EPS) dans le cadre de son contrat d'hébergement. Naturellement, Azure fournit des services Active Directory dans son cloud. En novembre 2018, AWS a annoncé un meilleur niveau de granularité pour les permissions d'accès au cloud, ce qui implique moins de fuites pour les applications SaaS. La crainte à long terme est que les fournisseurs de services de cloud public complètent leur environnement hôte avec des solutions de détection des menaces (en réalité, cela est déjà en train de se produire). En février 2019, Microsoft a annoncé sa solution SIEM Microsoft Azure Sentinel basée sur le cloud. Amazon GuardDuty supervise ses environnements cloud afin de détecter les comportements anormaux.

L'EDR devient une alternative viable au SIEM, plus particulièrement sur ce secteur d'activité. Tandis que le SIEM apporte une perspective globale sur ce qu'il se passe sur tout le réseau, les fournisseurs de solutions d'EDR apportent une visibilité sur les terminaux. Les solutions d'EDR ont directement

accès à la mémoire et peuvent détecter les manipulations opérées sur les appareils sans mesure télémétrique depuis le SIEM.

FIGURE 4

Répartition du chiffre d'affaires mondial tiré des ventes de solutions SIEM par fournisseur sur le segment des entreprises de 1 000 à 2 499 employés en 2018



Source : IDC, 2019

Le fait qu'une entreprise soit de petite taille ne signifie pas qu'elle passe inaperçue aux yeux des personnes malveillantes et sans scrupules. Par ailleurs, de nombreuses grandes entreprises disposent de centrales d'achat secondaires pour leurs bureaux régionaux. Les informations identifiables personnelles (PII) ou les numéros de carte de crédit sont précieux, quelle que soit la taille de l'entreprise, et doivent être protégés contre les vols.

En termes d'échelle et d'empreinte, les plateformes SIEM les plus importantes sont IBM QRadar et RSA NetWitness qui restent inaccessibles aux entreprises de cette taille. Celles-ci sont confrontées à des limites liées au nombre de solutions de cybersécurité qu'elles peuvent acheter et au nombre d'experts qu'elles peuvent affecter à la sécurité. Dans ces entreprises, il est probable que le personnel informatique se charge également de la sécurité.

L'approche adoptée en matière de réponses aux incidents est tout simplement différente dans les petites entreprises (voir Figure 5). Il est plus facile et rapide de s'appuyer sur des protocoles de reprise après sinistre que de réinitialiser des machines ou leur appliquer des correctifs.

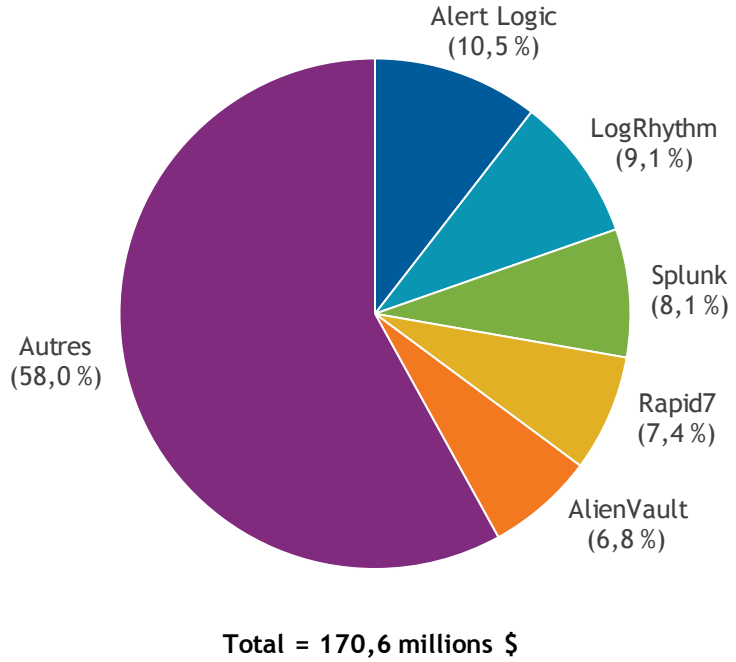
Jusqu'à mi-2017, les fournisseurs de solutions SIEM concevaient des appliances physiques tout-en-un qui protégeaient les serveurs en ligne. LogRhythm proposait un dispositif tout-en-un, et AlienVault

consolidait son appliance Unified Security Management (USM). Bien que ces appliances existent toujours, même AlienVault consacre ses efforts au cloud. L'attrait pour la communauté est un élément important qui caractérise les petites entreprises, et AlienVault OSSIM (une solution SIEM open source), ainsi que SolarWinds avec son réseau THWACK, permettent aux utilisateurs de partager des données et des approches tactiques.

Alert Logic est probablement le leader des solutions SIEM pour les entreprises de 1 à 999 employés, et nous nous attendons à ce qu'AlienVault gagne du terrain sur ce segment. SolarWinds Securonix se pose en challenger dans cette catégorie grâce à la possibilité de prendre en charge des déploiements de faible envergure.

FIGURE 5

Répartition du chiffre d'affaires mondial tiré des ventes de solutions SIEM par fournisseur sur le segment des entreprises de 1 à 999 employés en 2018



Total = 170,6 millions $

Source : IDC, 2019

L'ACTEUR QUI A COMPTÉ CETTE ANNÉE

Comme mentionné dans notre résumé, les fournisseurs de solutions SIEM sont en concurrence avec d'autres fournisseurs de solutions SIEM, et doivent rivaliser avec des acteurs externes à ce marché proposant des solutions gérées de détection et de réponse, des produits d'analyse de données et de veille économique ainsi que des plateformes open source. Tandis que la concurrence fait rage, les fournisseurs de solutions SIEM présentés dans les sections qui suivent ont une longueur d'avance, du moins pour le moment.

Splunk

Dans son rapport intitulé *The State of Dark Data* (l'état des données potentiellement utiles), Splunk a publié une donnée statistique intéressante. En moyenne, 55 % des données sont collectées et stockées, puis ne refont jamais surface. Une chose est sûre, Splunk a toujours voulu utiliser tout ce qui pouvait l'être. De son point de vue, des données inutilisées sont des possibilités inexploitées.

Lors de sa conférence en 2018, Splunk a annoncé les améliorations suivantes pour ses produits de sécurité :

- **Splunk Enterprise Security (ES) 5.2.** L'annonce du « séquençage d'événements » a été une amélioration importante apportée à Splunk ES 5.2. Splunk ES peut traiter une série d'événements importants et les corréler avec des modificateurs de risque pour réduire le nombre d'alertes et apporter aux analystes des SOC une visibilité sur le type d'attaque qui a lieu.
- **Phantom 4.1.** La profondeur de la plateforme d'orchestration Phantom est impressionnante – elle prend en charge 230 applications et 1 200 API. Phantom offre également une couche d'abstraction – ce qui signifie que si une entreprise décide de passer d'un pare-feu CISCO de nouvelle génération à un pare-feu Palo Alto, elle pourra le faire sans devoir réécrire ses scénarios d'automatisation.
- **Splunk UBA 4.2.** Au cours de la plupart des attaques, à un moment donné, la personne malveillante trouve les informations d'identification des utilisateurs légitimes et/ou crypte les données d'exfiltration. Splunk UBA crée une version de référence pour chaque utilisateur du réseau et compare les activités en temps réel aux comportements historiques. Pour superviser les comportements des utilisateurs finaux, Splunk UBA peut traiter 80 000 événements par seconde et superviser jusqu'à un million d'appareils. Enfin, le nouveau connecteur Splunk to Kafka UBA envoie des données directement à Kafka, sans passer par une instance de distribution des recherches, ce qui décuple les performances d'ingestion.

L'environnement de développement ARF (Adaptative Response Framework) de Splunk est à la base de Splunk ES. L'ARF offre des possibilités d'intégration avec plus de 50 fournisseurs de solutions de sécurité. Il permet de construire des corrélations, d'examiner les incidents et d'effectuer des audits des réponses permettant aux analystes de gérer les flux de travail et de procéder à une double vérification des actions dans des domaines spécifiques.

On peut considérer que le meilleur argument en faveur de Splunk réside dans le grand nombre de plateformes différentes que l'entreprise déploie pour l'informatique et l'IoT, ainsi que le confort d'utilisation pour les administrateurs informatiques. Sur le plan informatique, Splunk propose des fonctionnalités de supervision des applications, de suivi des infrastructures, de suivi de la virtualisation et d'analyse prédictive permettant à la plateforme d'anticiper les mises à jour de maintenance des différents appareils.

L'Université d'État de l'Arizona a présenté un cas d'usage très particulier. L'administrateur des systèmes s'occupait des achats pour l'université et pensait qu'il ferait des économies d'échelle en unifiant l'administration de la base de données RH, du réseau et d'autres bases de données sur une plateforme Splunk. Il était convaincu que la segmentation des données pourrait aisément être prise en charge par des applications tierces et, même sans une parfaite harmonisation, il estimait qu'il gagnerait en efficacité si tous les employés de chaque département utilisaient le même outil. Les résultats obtenus ont été conformes à ses attentes.

Splunk a constamment augmenté son chiffre d'affaires de 35 à 40 % chaque année au cours des quatre dernières années. Cependant, son offre considérée comme le meilleur moteur d'ingestion de données pour la sécurité et les analyses est menacée par d'autres entreprises telles que Securonix et Exabeam qui s'appuient sur différentes formes de collecte de données Apache (Hadoop et Kafka) et appliquent une couche analytique aux lacs de données. SAP commence à s'intéresser au SIEM et même les plateformes de veille économique (BI) traditionnelles, telles que BMC Software, pourraient faire leur introduction sur le marché des analyses de sécurité.

CONTEXTE DU MARCHÉ

Les évolutions importantes du marché

Les préoccupations d'ordre concurrentiel, technique et marketing touchant les fournisseurs de solutions SIEM ont été exposées tout au long de ce document, mais il reste quelques questions à aborder.

Il y a peu de temps encore, les plateformes d'automatisation et d'orchestration étaient soit des éléments autonomes, soit des éléments essentiels du SIEM. En 2016, Rapid7 a racheté Kommand. En 2017, IBM a racheté Resilient pour l'orchestration des réponses aux incidents, et en avril 2018 Splunk a racheté Phantom. En février 2019, Palo Alto Networks a fait part de ses intentions, puis a racheté Demisto. Il s'agit d'une évolution intéressante dans le domaine de la cybersécurité. En 2018, Palo Alto Networks a racheté Secdo, Evident.io et Redlock pour se doter de capacités d'EDR et acquérir une notoriété en matière de technologies cloud. Palo Alto Networks fait désormais valoir de solides capacités de détection des menaces grâce à WildFire, qui permet de détecter les malwares, et à Cortex XDR qui analyse le trafic sur le réseau et les terminaux. Où en sont d'autres entreprises, telles que Tenable et Qualys, dans l'unification de capacités technologiques disparates ? Les plateformes d'automatisation et d'orchestration se rapprocheront-elles des plateformes d'UBA qui sont des technologies sous-jacentes, quasiment communes et jouant un rôle de soutien pour les analyses de sécurité, l'EDR et le SIEM ? Vraisemblablement, d'autres sujets concernant la cybersécurité sont d'actualité, et ils pourront atténuer ou renforcer l'importance du SIEM. IDC s'attend à ce que les cyberassureurs établissent des listes de contrôle quasi-inédites des exigences en matière d'assurance. Ces listes de contrôle pourraient prévoir :

- Une déduction de 5 % de la prime d'assurance si l'assuré utilise l'environnement de développement MITRE ATT&CK.
- Une déduction de 7 % de la prime d'assurance si l'assuré respecte les exigences de la publication NIST 800.53 concernant la déclaration mensuelle de l'ensemble de ses actifs et dispositifs numériques.
- Une déduction de 10 % si l'assuré est en mesure de démontrer que ses délais de réponse aux alertes critiques ne dépassent pas 24 heures en moyenne.

La deuxième préoccupation principale concerne les organismes gouvernementaux de réglementation. Le RGPD et les prochaines lois California Privacy Laws sont mis en œuvre. Les conditions dans lesquelles ces organismes pourront imposer des amendes et les recours disponibles pour les entreprises sont toujours en cours d'établissement. Tandis que l'accent a surtout été mis sur l'identité et la souveraineté des données, le poids d'une négligence évidente intervenant dans les pratiques de cybersécurité et contribuant à une violation n'a pas encore été ouvertement plaidé à l'occasion d'un litige.

MÉTHODOLOGIE

L'évaluation de la taille du marché des logiciels et les prévisions d'IDC se fondent sur le chiffre d'affaires tiré des logiciels commerciaux. IDC utilise le terme *logiciels commerciaux* pour distinguer les logiciels disponibles dans le commerce des logiciels développés spécifiquement. Les logiciels commerciaux sont des programmes ou des ensembles de codes de tout type disponibles dans le commerce par voie de vente, de location, de crédit-bail ou en tant que service. Le chiffre d'affaires tiré de ces logiciels commerciaux regroupe typiquement les montants initiaux et réguliers facturés en contrepartie du droit d'utilisation accordé par les licences de ces logiciels. Dans le cadre des contrats de licence, ces montants peuvent couvrir un accès à l'assistance produit et/ou à d'autres services indissociablement liés à chaque licence d'utilisation spécifique, ou le support peut être facturé séparément. Les mises à jour peuvent être comprises dans le droit d'utilisation permanent ou être facturées séparément. Les logiciels commerciaux doivent être disponibles dans le cadre d'appels d'offres. Ces cas d'usage sont pris en compte par IDC dans le chiffre d'affaires tiré des ventes des logiciels commerciaux.

Le chiffre d'affaires tiré des ventes de logiciels commerciaux ne tient pas compte des services facturés pour la formation, le conseil et l'intégration des systèmes qui ne sont pas couverts par le droit d'utilisation accordé par la licence (ou sont dissociés de la licence), mais il tient compte de la valeur implicite des logiciels incluse dans les services offrant des fonctionnalités logicielles soumises à un barème tarifaire différent. Le total du chiffre d'affaires tiré des ventes de logiciels commerciaux ainsi calculé est ensuite réparti entre les marchés, les zones géographiques et, dans certains cas, les environnements d'exploitation. Pour obtenir plus d'informations, voir le document *IDC's Worldwide Software Taxonomy, 2018: Update* (Taxonomie mondiale 2018 d'IDC pour les logiciels : actualisation) (IDC N° US44835319, février 2019)

Pour 2018, la collecte de données de bas en haut et au niveau de toute l'entreprise a commencé en janvier 2019, mais une précédente phase de collecte a commencé en septembre 2018 pour l'année 2017. Il a été demandé aux fournisseurs d'indiquer leur chiffre d'affaires selon la taille des entreprises clientes, les différentes formes de plateformes, les régions géographiques et les secteurs d'activités (cette étude présente les données sur les parts de marché global et la taille des entreprises). La taille des entreprises est évaluée en tenant compte de leur taille totale et non de celle de centrales d'achat individuelles. Les montants des chiffres d'affaires présentés dans cette étude sont essentiellement issus des résultats de l'enquête ; toutefois, les déclarations 10-Q et 10-K des rapports publics ont été prises en considération, tout comme les données provenant du suivi des logiciels d'IDC (IDC Software Tracker). Toutes les entreprises n'ont pas répondu directement, et IDC ne formulera aucun commentaire concernant une entreprise en particulier.

Les données présentées dans cette étude sont des estimations d'IDC exclusivement.

Remarque : l'ensemble des chiffres figurant dans ce document peut ne pas être tout à fait exact en raison des arrondis.

DÉFINITION DU MARCHÉ

Les solutions de gestion des événements et des informations de sécurité (SIEM) comprennent des produits conçus pour agréger des données issues de multiples sources afin de pouvoir identifier des schémas d'événements susceptibles d'indiquer une attaque, une intrusion, une utilisation abusive ou une défaillance. La mise en corrélation des événements simplifie et accélère le suivi des événements

sur le réseau en consolidant les alertes et les enregistrements d'erreurs au sein d'un paquet concis et facile à interpréter. Ces produits peuvent également consolider et stocker les données de journaux ayant été traitées par la solution SIEM. Ce segment de marché comprend également les produits qui collectent et diffusent des renseignements sur les menaces, offrent des services d'alertes précoces sur les menaces et sont capables de fournir des informations sur les contre-mesures. Les données issues des produits SIEM sont transmises aux solutions gérant les politiques et la conformité afin d'établir des rapports cohérents.

Cette définition formelle du SIEM revêt une réelle importance pour plusieurs raisons et principalement pour des motifs de transparence. Ce terme peut paraître imprécis, mais l'un des critères permettant de considérer qu'une plateforme est de type SIEM repose sur sa capacité à se comporter comme telle. Une solution de SIEM doit prendre en compte différents journaux et flux, disposer de tableaux de bord spécifiquement utilisés pour les enquêtes sur les menaces, et elle doit être capable de fournir des rapports de conformité. En ce sens, une solution SIEM se différencie des produits d'analyse de sécurité conçus dans le but d'offrir de la flexibilité aux utilisateurs pour spécifier leur cadre de sécurité particulier et exploiter les données en fonction de ce cadre, et améliorer ainsi les analyses des données ; Darktrace et Anomali font partie de ces produits. Par ailleurs, les solutions SIEM se différencient des produits de veille sur les menaces conçus pour tenir compte de diverses sources de renseignement sur les menaces et fournir aux entreprises une plateforme leur permettant d'analyser leurs propres données au regard de nombreuses sources de renseignement variées. Souvent, les entreprises utilisent des plateformes de veille économique (BI) en association avec des plateformes open source pour indexer les données, mais IDC n'en tient pas compte dans le chiffre d'affaires lié aux solutions SIEM. Dans l'idéal toutefois, une solution SIEM devrait intégrer des aspects liés aux analyses de la sécurité et des menaces, à la veille sur les menaces, à la veille économique et à la gestion des bases de données afin de pouvoir fournir des capacités de recherche, de stockage, d'indexation et surtout, des données qui facilitent les détections et les réponses aux incidents.

ÉTUDES EN RAPPORT AVEC LE PRÉSENT DOCUMENT

- *IDC Market Glance: Cybersecurity AIRO, 1Q19* (Aperçu du marché selon IDC : analyses, renseignement, réponses et orchestration en matière de cybersécurité (IDCN° US44774119, février 2019)
- *Market Analysis Perspective: Worldwide Cybersecurity AIRO, 2018 - Harden, Detect, Respond, and Repeat* (Perspective de marché : analyses, renseignement, réponses et orchestration en matière de cybersécurité – renforcer, détecter, répondre et répéter (IDC N° US44282118, septembre 2018)
- *Worldwide IT Security Products Forecast, 2018-2022: Do You Make Friends or Acquire Technology to Round Out a Portfolio? (Prévisions mondiales concernant les produits de sécurité informatique, 2018-2022 : cherchez-vous à créer des liens ou à acquérir des solutions technologiques pour renforcer un portefeuille ?* (IDC N° US44182918, août 2018)
- *Worldwide Security and Vulnerability Management Forecast, 2018-2022: SVM Vendors Fight Off New Market Entrants (Prévisions mondiales concernant la gestion de la sécurité et des vulnérabilités, 2018-2022 : les fournisseurs de solutions de SVM luttent contre les nouveaux entrants sur le marché* (IDC N° US43491618, juillet 2018)
- *Worldwide Security and Vulnerability Management Market Shares, 2017: Defending the Boundaryless Network* (Parts du marché mondial de la gestion de la sécurité et des vulnérabilités, 2017 : défendre le réseau sans frontière (IDC N° US42049417, juillet 2018)

- *Worldwide Security as a Service Market Shares, 2017: The Sweet Spot Between DIY and Managed Services* (Parts du marché mondial de la sécurité as a service, 2017 : le parfait équilibre entre une prise en charge en interne et les services gérés (IDC N° US44016818, juin 2018)

À propos d'IDC

International Data Corporation (IDC) est le premier fournisseur mondial d'informations sur les marchés commerciaux, de services de conseil et d'événements sur la technologie de l'information, les télécommunications et les marchés des technologies pour le grand public. IDC aide les professionnels de l'informatique, les dirigeants d'entreprise et la communauté des investisseurs à prendre des décisions qui se fondent sur des faits pour les acquisitions technologiques et la stratégie de l'entreprise. Plus de 1 100 analystes d'IDC apportent une expertise mondiale, régionale et locale sur les questions d'opportunités technologiques et sectorielles, ainsi que sur les tendances qui se dégagent dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC fournit des informations approfondies stratégiques afin d'aider ses clients à atteindre leurs objectifs commerciaux clés. IDC est une filiale d'IDG, la principale société en matière de médias, de recherche et d'événements liés à la technologie.

Siège social mondial :

5 Speen Street
Framingham, MA 01701
États-Unis
+1.508.872.8200
Twitter : @IDC
idc-community.com
www.idc.com