Les 5 tendances du SIEM à surveiller en 2022

splunk>
turn data into doing®

La gestion des événements et incidents de sécurité (SIEM) s'est bien installée dans le paysage : les fonctions fondamentales de la plateforme remontent à plus d'une dizaine d'années. Depuis, les solutions SIEM, qui étaient au départ de simples outils de gestion des logs, sont devenues de véritables plateformes d'information, et ce sont les exigences des entreprises en matière de sécurité qui façonnent le plus le marché du SIEM. Ne serait-ce qu'au cours des dernières années, le marché du SIEM a augmenté de façon stupéfiante, passant de 2 milliards de dollars à 4,1 milliards de dollars.

Les recherches menées par de grands analystes du marché ont également révélé que le coût des violations de données devrait dépasser 5 000 milliards de dollars d'ici 2024. C'est presque le *double* du montant déclaré en 2019, qui s'élevait à 3 000 milliards de dollars. Mais grâce aux nouvelles fonctionnalités du logiciel SIEM, les organisations peuvent atténuer ce type de risque et arrêter *davantage* de menaces (voire *toutes*) avant qu'elles ne provoquent des dommages considérables. Le Magic Quadrant de Gartner pour la Gestion des informations et des événements de sécurité met en évidence ces tendances à l'heure où les fournisseurs de logiciels SIEM continuent d'innover et d'itérer.

Face à tant de possibilités passionnantes à l'horizon, voici les **cinq tendances du SIEM à surveiller en 2022 :**

1. La sécurité du cloud et des applications reste une grande priorité.
2. Les alertes basées sur les risques vont faire l'objet d'une attention renforcée.
3. La threat intelligence et les contenus de sécurité intégrés au produit sont désormais essentiels.
4. L'automatisation augmente l'efficacité, la productivité et la réactivité.
5. Les menaces internes seront plus faciles à identifier et à prendre en charge.

01

La sécurité du cloud et des applications reste une priorité de haut niveau

Avec l'adoption croissante du cloud, en grande partie due au COVID-19 et au passage massif au télétravail, toutes les entreprises, grandes et petites, ont été contraintes d'adopter une solution de sécurité moderne. Les entreprises adoptent les infrastructures cloud à un rythme soutenu, et n'ont d'autre choix que de mettre en œuvre et moderniser leur stratégie cloud dans les meilleurs délais.

Les complexités techniques de la migration ne sont qu'un des nombreux défis auxquels elles seront confrontées lors du passage au « cloud-native ». Les équipes, fonçant tête baissée avec les initiatives numériques, ont tendance à négliger les obligations de sécurité générales dans le but de devancer la concurrence et de s'adapter à l'évolution des priorités. Tout cela entraîne une augmentation globale du risque, en particulier si l'entreprise n'est pas à jour en termes de contrôle du réseau, de système de gestion des accès ou d'options de configuration.

Ajoutez à cela l'élargissement de la surface d'attaque et le manque de visibilité, et vous comprenez l'imminence de la menace. C'est pour cela qu'une solution SIEM robuste doit être fournie avec du contenu de supervision de sécurité cloud prêt à l'emploi pour faciliter la détection et la prise en charge des menaces dans les environnements hybrides, cloud et multicloud. Il faut également des règles de détection sophistiquées pour les attaques dans le cloud, assorties d'une large gamme de méthodes d'attaque pour tester et améliorer en permanence la détection

À l'ère du travail à distance, une solution SIEM doit être capable de capturer et d'analyser toutes les données du cloud et des terminaux, quels que soient leur volume, leur variété et leur vitesse. La supervision traditionnelle ne suffit plus ; les équipes de sécurité doivent analyser et ingérer des données provenant d'un large éventail de sources, dans tous les types d'environnements, afin de comprendre les tenants et les aboutissants des événements de sécurité.

02

Les alertes basées sur les risques vont faire l'objet d'une attention renforcée

Les analystes sont toujours accablés par un déluge d'alertes quotidiennes. Les alertes reposant sur des détections aux définitions larges peuvent entraîner un gros volume de faux-positifs, générer beaucoup de bruit dans le centre des opérations de sécurité (SOC), et ainsi submerger rapidement le personnel de première ligne.

Sans surprise, les SIEM doivent devenir plus performants et efficaces dans la détection et la prise en charge des attaques ciblées et des violations. Les alertes basées sur les risques (RBA) en particulier, une nouvelle méthodologie d'identification des menaces, attribuent un niveau de risque aux utilisateurs et aux entités, et déclenchent une alerte lorsque certains seuils de comportement et de risque sont franchis.

Les équipes de sécurité peuvent alors réduire le volume d'alertes (et augmenter la proportion de vrais positifs) en mettant en évidence les attaques sophistiquées souvent ignorées par les recherches traditionnelles.

Dans un SIEM, ce type de profilage des comportements, de threat intelligence et d'analyse peut considérablement améliorer la performance de la détection, en libérant du temps et des ressources pour les consacrer aux menaces haute-fidélité complexes. Les analystes peuvent également attribuer un risque à diverses entités en fonction du framework de cybersécurité standard qu'ils ont choisi, comme MITRE ATT&CK, NIST, etc.

03

La threat intelligence et le contenu de sécurité intégré au produit sont désormais indispensables

Maintenir et faire évoluer les règles d'un programme de sécurité n'a rien de simple. Avec une telle variété de sources, de structures et de formats à traiter, l'exploitation des informations, pourtant indispensable, devient fastidieux et chronophage, *surtout* lorsque les équipes de sécurité n'ont quasiment aucune marge pour créer les détections et les playbooks nécessaires.

Mais de nos jours, une solution SIEM moderne peut intégrer de la threat intelligence (des recherches de sécurité intégrées au produit concernant les menaces existantes et émergentes) à chaque étape du flux de réponse aux incidents, ainsi qu'à travers un écosystème d'équipes, d'outils, de pairs et de partenaires. Les conseils fournis aident les utilisateurs à anticiper les attaques et à créer des pipelines complexes sans jamais avoir à écrire ou à gérer des scripts en back-end.

Enfin, grâce à la croissance rapide du marché de l'intelligence, qui englobe tous les types de sources d'informations ouvertes, commerciales et communautaires, les solutions SIEM sont plus à même d'intégrer les derniers conseils techniques et les informations de contexte (les responsables de l'attaque et leurs techniques, notamment) qui guident les analystes dans l'investigation et la prise en charge d'une alerte.

04

L’automatisation augmente l’efficacité, la productivité et la réactivité

Certaines tâches de sécurité sont tout simplement trop volumineuses et fastidieuses pour être traitées manuellement par les équipes. N’oublions pas non plus que la pénurie de talents en cybersécurité permet difficilement de trouver (sans même parler de recruter) assez de personnes pour la charge de travail d’une entreprise. Sans surprise, les analystes risquent le burn-out tandis que des menaces prioritaires passent inaperçues. Pour maximiser la productivité, l’efficacité et la rapidité, sans mettre en danger la santé mentale de quiconque, la seule voie à suivre est l’automatisation.

C’est là qu’interviennent les solutions d’orchestration, d’automatisation et de réponse de sécurité (SOAR). Désormais, on attend de la plupart des solutions SIEM qu’elles intègrent des capacités SOAR pour prendre en charge les tâches fastidieuses des analystes et résoudre les incidents de sécurité en un temps record, afin de faire passer le temps de réponse de plusieurs minutes (voire plusieurs heures) à quelques secondes. Un outil SOAR y parvient en unifiant les informations issues de plusieurs outils, en enrichissant les données d’alerte et en les faisant apparaître dans une interface unique. En automatisant le processus de collecte de données, l’analyste peut voir des détails précieux sur l’alerte dès qu’elle apparaît.

En conclusion ? L’orchestration et l’automatisation aident les équipes de sécurité à mener des investigations et à répondre aux alertes de sécurité beaucoup plus rapidement, et enrichissent également les données qu’elles collectent en compilant en un même endroit des informations provenant de sources variées. En orchestrant les décisions et les actions pour analyser, trier et prendre rapidement en charge un volume élevé d’alertes, les équipes de sécurité peuvent rapidement déterminer le niveau de risque et réagir en conséquence.

05

Les menaces internes seront plus faciles à identifier et à combattre

Comme les menaces internes sont les plus difficiles à détecter (et sans doute les plus nuisibles), l'analyse du comportement des entités et des utilisateurs (UEBA) s'avère vitale pour détecter les tendances suspectes pouvant indiquer un vol d'identifiants, une fraude ou autre activité malveillante. Fondamentalement, l'UEBA identifie et suit les comportements des acteurs menaçants au fil de leur parcours dans les environnements d'entreprise, en traitant les données à l'aide d'une série d'algorithmes qui détectent les activités déviant des normes d'utilisation.

Traditionnellement, l'UEBA était adoptée dans le cadre d'une approche progressive ; les organisations commençaient avec un SIEM de base, qu'elles élargissaient ensuite à l'UEBA et/ou au SOAR (et au-delà). Mais aujourd'hui, l'UEBA est considérée comme une fonctionnalité clé par Gartner et devrait fonctionner de concert, et idéalement de la manière la plus transparente possible, avec une solution SIEM pour fournir des informations sur les modèles de comportement au sein du réseau.

En combinant la puissance des deux technologies au sein d'une même plateforme, l'entreprise profite des avantages des techniques de détection des menaces examinant aussi bien le comportement des humains que celui des machines. En intégrant l'UEBA dans votre SIEM, vous êtes mieux armé pour reconnaître les anomalies comportementales et vous disposez d'un contexte plus riche autour des menaces connues et inconnues. Les analystes gagnent un temps précieux et votre équipe devient plus efficace grâce à l'élimination des faux positifs ; seules sont signalées les menaces haute-fidélité qui ne sont généralement pas détectées par une corrélation basée sur des règles.

Pour en savoir plus sur les tendances SIEM et les bonnes pratiques des leaders de la cybersécurité, consultez le *Magic Quadrant 2021 de Gartner*.

Recevoir le rapport

splunk>
turn data into doing®

22-22392-Splunk-Top 5 SIEM Trends to Watch in 2022-LS-104