IBM Security

Six mythes de la SIEM

IBM

Études des six mythes de la SIEM

Vous êtes-vous renseigné sur les solutions de SIEM récemment ? Parce que les choses ont changé dans ce domaine.

D'après la rumeur, les solutions de gestion de l'information et des événements de sécurité (SIEM, pour security information and event management) sont lourdes et complexes – et donc réservées aux grandes entreprises. Il est vrai que certaines d'entre elles le sont, mais ce mythe ne tient pas compte des solutions plus modernes qui sont conçues pour les entreprises de toute taille.

Ce n'est un secret pour personne que le secteur de la cybersécurité est confronté à une forte pénurie de compétences. Les solutions de sécurité (comme toutes les solutions) doivent donc être conçues pour vous permettre d'être efficace dans votre travail en dépit de vos ressources (probablement) limitées. Lorsque vous évaluez des solutions de SIEM modernes, recherchez celles qui autonomisent votre équipe de sécurité et qui vous permettent de tirer le meilleur parti des ressources dont vous disposez.

Nous allons nous intéresser aux six principaux mythes de la SIEM et déterminer ce que vous pouvez attendre aujourd'hui d'une solution de SIEM.

Mythe n° 1

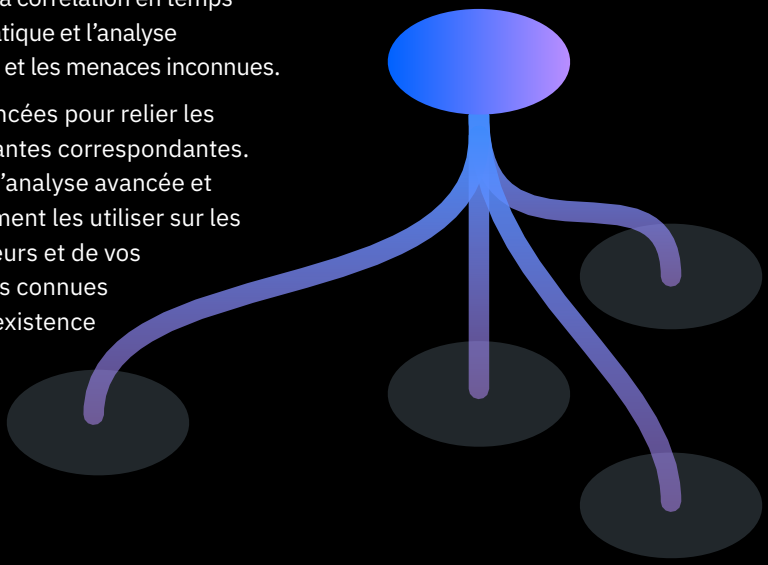
Une solution de SIEM ne peut détecter que les menaces connues ; elle n'est d'aucune aide pour les menaces inconnues.

Les solutions de SIEM n'utilisent que la corrélation pour détecter les menaces, et pour créer une règle de corrélation efficace vous devez d'abord savoir quoi rechercher.

La vérité

Les solutions de SIEM efficaces utilisent conjointement la corrélation en temps réel, la détection des anomalies, l'apprentissage automatique et l'analyse comportementale pour détecter les menaces connues – et les menaces inconnues.

Elles utilisent aussi des techniques de corrélation avancées pour relier les indices entre eux et comprendre les activités malveillantes correspondantes. Si votre solution de SIEM intègre des fonctionnalités d'analyse avancée et de corrélation en temps réel, vous pouvez immédiatement les utiliser sur les activités de votre réseau, de vos actifs, de vos utilisateurs et de vos applications pour détecter non seulement les menaces connues mais aussi les activités anormales pouvant indiquer l'existence de menaces inconnues.



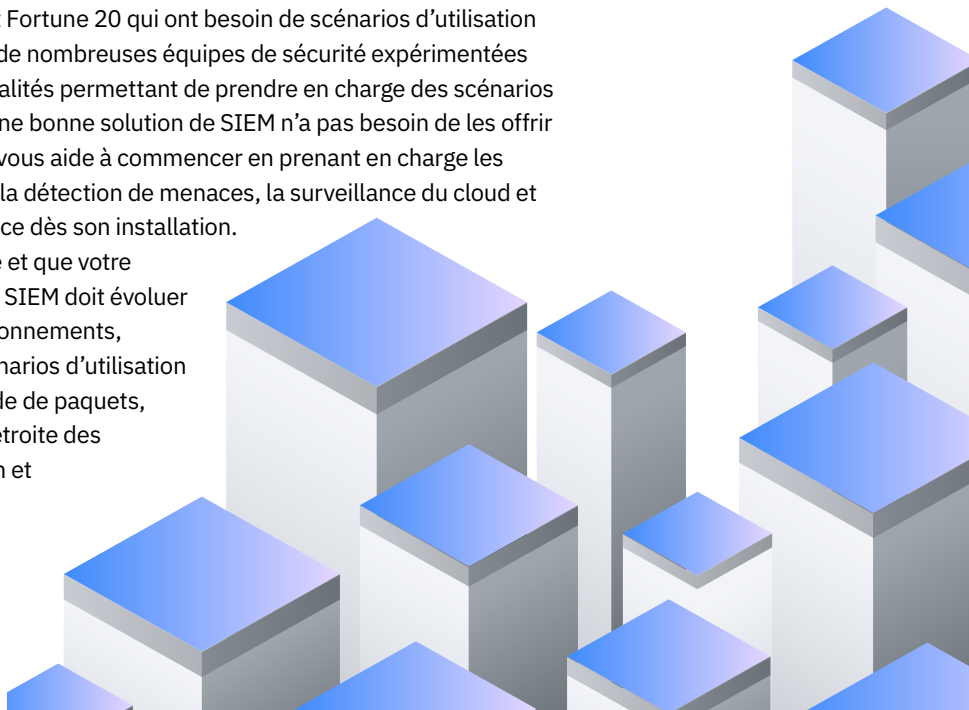
Mythe n° 2

Les solutions de SIEM sont réservées aux grandes entreprises disposant d'équipes de sécurité expérimentées.

Selon l'opinion communément admise, puisque les meilleures solutions de SIEM du marché sont capables de supporter les plus grandes entreprises, elles ne s'adressent qu'à celles-ci.

La vérité

Les meilleures solutions de SIEM s'adressent à une grande variété d'entreprises, que ce soit les entreprises en croissance qui commencent seulement à surveiller leur sécurité ou les entreprises internationales du classement Fortune 20 qui ont besoin de scénarios d'utilisation sophistiqués. La vérité, c'est qu'alors que de nombreuses équipes de sécurité expérimentées préfèrent disposer de toutes les fonctionnalités permettant de prendre en charge des scénarios d'utilisation spécifiques et sophistiqués, une bonne solution de SIEM n'a pas besoin de les offrir toutes pour être utile. Une solution idéale vous aide à commencer en prenant en charge les scénarios d'utilisation standards, tels que la détection de menaces, la surveillance du cloud et la création de rapports de conformité – et ce dès son installation.
À mesure que vous prenez de l'expérience et que votre entreprise se développe, votre solution de SIEM doit évoluer pour prendre en charge davantage d'environnements, plusieurs zones géographiques et des scénarios d'utilisation sophistiqués, tels que l'inspection profonde de paquets, l'analyse du trafic DNS et une intégration étroite des outils SOAR (orchestration, automatisation et réponse dans le domaine de la sécurité).



Mythe n° 3

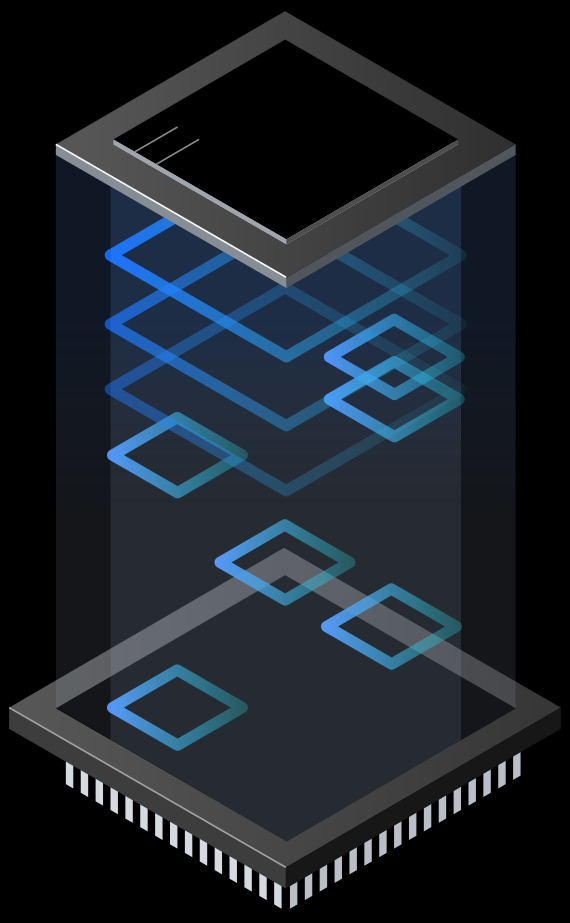
Les solutions SIEM ont besoin de beaucoup de données, et le coût de leur collecte est extrêmement élevé.

Les prix de certains fournisseurs étant réputés pour devenir très vite prohibitifs, certaines équipes de sécurité supposent qu'il en va de même pour toutes les solutions de SIEM.

La vérité

Si vous incluez dans votre étude les fournisseurs qui facturent au volume de données stockées, sachez que ce mode de facturation peut très vite devenir très onéreux. Toutefois, naturellement, les prix des solutions diffèrent selon les fournisseurs.

Avant de vous engager, réfléchissez aux problèmes que vous souhaitez résoudre : êtes-vous un détaillant qui doit protéger des données de cartes de paiement ? Avez-vous besoin de visibilité sur Amazon Web Services car votre entreprise migre vers ce nouvel environnement ? Les données que vous collectez aux fins de sécurité devront vous aider à traiter vos propres scénarios d'utilisation. Ne vous laissez pas convaincre de tout analyser si vous n'en avez pas besoin. Cela dit, si la réglementation ou vos politiques internes vous imposent de conserver certaines données, il faudra que votre fournisseur de solutions de SIEM puisse vous proposer une option peu onéreuse limitée au stockage, à la recherche et à la génération de rapports. En analysant uniquement ce qui est important pour votre entreprise et en envoyant le reste de vos données d'historiques et d'événements vers un système de stockage à faible coût, vous pouvez mener à bien un projet de SIEM sans qu'il engloutisse la totalité de votre budget.



Mythe n° 4

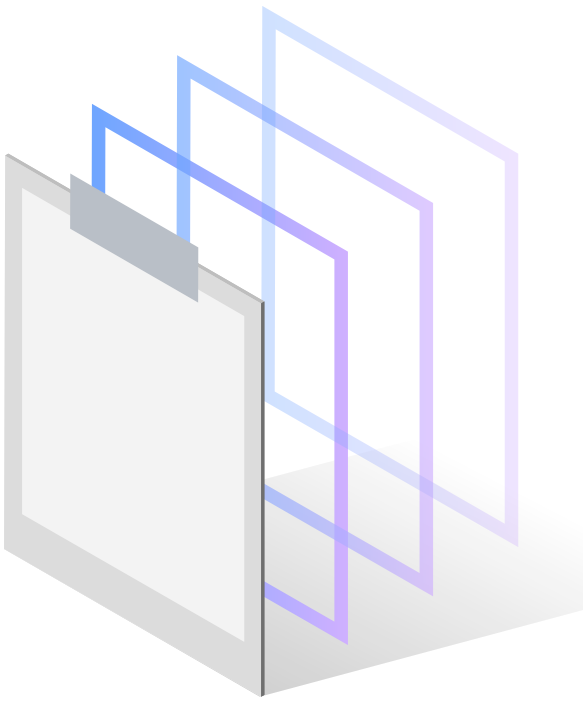
Pour que votre solution de SIEM soit efficace, vous avez besoin d'une équipe de spécialistes des données travaillant à plein temps à sa gestion.

On dit souvent que pour qu'une solution de SIEM soit efficace, il faut qu'un spécialiste des données (ou une équipe de ces spécialistes) travaille à plein temps à la création ex nihilo de toutes ses règles et analyses.

La vérité

Si vous ne pouvez pas (ou ne souhaitez pas) mettre sur pied et payer une équipe de spécialistes des données maîtrisant également le domaine de la sécurité, recherchez un fournisseur qui propose du contenu prêt à l'emploi avec sa solution.

Certains fournisseurs partent du principe que puisque de toute façon la solution sera probablement personnalisée, pourquoi ne pas partir de rien. Aujourd'hui, en pratique, les équipes de sécurité ne disposent tout simplement pas des ressources nécessaires pour s'attaquer à un projet aussi énorme et qui requiert des compétences aussi pointues. Toutes les solutions de SIEM vous demanderont de leur fournir des informations concernant votre réseau ; mais cela fait, vous devriez pouvoir tirer parti de règles, d'analyses et de politiques de corrélation prédéfinies pour commencer immédiatement à détecter les menaces. Vous ne devriez pas être obligé de partir de zéro. Et si vous avez encore des inquiétudes à ce sujet, sachez que de nombreux fournisseurs de solutions de SIEM se sont associés avec des prestataires de services de sécurité managés pour vous permettre de bénéficier de tous les avantages d'une solution de SIEM moderne et, en cas de besoin, de l'aide de spécialistes de la sécurité.



Mythe n° 5

Une pile de gestion de journaux peut offrir la même visibilité qu'une solution de SIEM.

Le marketing créatif des fournisseurs de solutions de gestion de journaux et de lacs de données voudrait vous faire croire que les solutions de gestion de journaux sont meilleures que les solutions de SIEM pour détecter les menaces et mener les investigations qui s'imposent.

La vérité

Les outils de gestion de journaux conviennent très bien pour tout ce qui a trait à la conformité et aux audits, mais ils ne donnent pas de bons résultats dans les domaines de l'analyse et des alertes en temps réel.

Les outils de gestion de journaux ont été créés pour résoudre un problème qui était vieux de dix ans : à l'époque, les entreprises avaient besoin de solutions leur permettant, en cas d'audit, de prouver leur conformité à la loi Sarbanes-Oxley (SOX), à la norme Payment Card Industry (PCI) et à d'autres réglementations sectorielles. Ces dernières années, les piles de gestion de journaux ont connu un regain d'intérêt suite à des affirmations vantant leur capacité à explorer et indexer des pétaoctets de données. Toutefois, l'absence de fonctionnalité d'analyse en temps réel dans ces outils place sur les épaules de votre personnel – déjà limité – des responsabilités disproportionnées en matière de détection manuelle – aussi bien pour l'interrogation que la réorientation ou la recherche de menaces.

La plupart des fournisseurs de solutions de SIEM incluent une couche de gestion de journaux ou un lac de données dans leur solution, aux fins d'agrégation, d'analyse syntaxique et de stockage. Souvent, cette couche de gestion de journaux fait l'objet d'une licence distincte de celle de la solution de SIEM, ce qui permet aux équipes de créer un lac de données de sécurité en bénéficiant d'un modèle de tarification abordable et prévisible, car basé sur l'hôte. La valeur ajoutée de la solution de SIEM réside dans sa fonctionnalité d'analyse (corrélation en temps réel, apprentissage automatique, etc.) prête à l'emploi, qui effectue le plus gros du travail de surveillance et de détection. En résumé, un outil de gestion de journaux ne constitue pas à lui seul une solution de SIEM, il n'est qu'une fonctionnalité d'une solution de SIEM.

Mythe n° 6

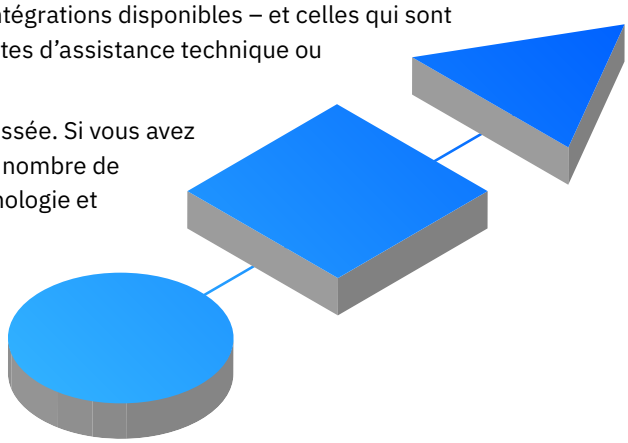
Dans mon environnement, il est difficile d'intégrer les solutions de SIEM avec les autres solutions.

Les solutions de SIEM ont la réputation d'être difficiles à intégrer avec d'autres solutions, alors même qu'elles font appel aux données d'autres solutions pour fonctionner.

La vérité

Les principales solutions de SIEM doivent être faciles à intégrer – et heureusement beaucoup d'entre elles le sont.

Parmi les premières solutions de SIEM qui ont été commercialisées il y a dix ans, celles qui n'ont pas évolué en même temps que les besoins et la technologie sont effectivement difficiles à intégrer. Cependant, aujourd'hui, ces acteurs ont complètement disparu ou sont en grande difficulté. Aujourd'hui, les principales solutions offrent des centaines d'intégrations prêtes à l'emploi avec les technologies informatiques (IT) et opérationnelles (OT) commerciales, ainsi que des connecteurs simples permettant de les intégrer avec des applications personnalisées afin de pouvoir analyser leurs journaux. Si vous voulez connaître les intégrations disponibles – et celles qui sont intégralement prises en charge par les fournisseurs –, consultez les sites d'assistance technique ou d'échange d'applications des fournisseurs.



Les stéréotypes actuels sont souvent basés sur une technologie dépassée. Si vous avez évalué une solution de SIEM il y a dix ans – ou même cinq –, un grand nombre de ces principaux mythes étaient alors fondés. Mais tout comme la technologie et les menaces, les solutions de SIEM ont évolué.

Si vous rencontrez des difficultés pour détecter les menaces ou interpréter les journaux dans votre gestionnaire de journaux, il est peut-être temps de vous intéresser de nouveau aux solutions de SIEM et de découvrir par vous-même combien elles ont changé.

A propos d'IBM Security QRadar

Renforcez vos défenses pour contrer l'augmentation des menaces en choisissant IBM Security QRadar, la solution de gestion de l'information et des événements de sécurité (SIEM) de pointe. Faites évoluer et mettez à l'échelle vos opérations de sécurité avec les outils intégrés de visibilité, de détection, d'investigation et de réaction. Bénéficiez d'une visibilité complète sur votre environnement et utilisez l'analyse avancée pour prioriser vos menaces les plus graves. Avec QRadar, vous pouvez monter en puissance rapidement grâce à la prise en charge intégrée de milliers d'intégrations et de scénarios d'utilisation couvrant tous les aspects de la sécurité. Détectez les menaces en temps réel grâce aux fonctionnalités d'analyse avancée et de renseignement sur les menaces, qui s'appuient sur le savoir-faire étendu que nous avons acquis au fil des ans en protégeant des entreprises du classement Fortune 100. QRadar peut vous aider à accélérer votre mise en conformité et à gérer le risque réglementaire grâce à sa prise en charge des réglementations RGPD, ISO 27001, HIPAA, etc. Tirez parti d'IBM Watson pour démultiplier l'efficacité de vos équipes de sécurité grâce aux investigations assistées par l'IA qui priorisent et automatisent le tri et permettent des enquêtes jusqu'à 60 fois plus rapides. Enfin, réagissez aux menaces plus vite et de façon plus efficiente grâce à l'orchestration, à l'automatisation, à la gestion des cas et aux livrets de jeu dynamiques fournis par l'intégration étroite avec IBM Security SOAR.

Pour en savoir plus, consultez la page web **ibm.com/qradar**.

IBM Security

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse suivante :
ibm.com

Le présent document contient des informations en vigueur à la date de la première publication et susceptibles d'être modifiées par IBM à tout moment. Toutes les offres mentionnées ne sont pas distribuées dans tous les pays où IBM exerce son activité.

Les données de performances et les exemples de clients ne sont présentés qu'à des fins d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation spécifiques.

LES INFORMATIONS DU PRÉSENT DOCUMENT SONT FOURNIES « EN L'ÉTAT » ET SANS GARANTIE EXPLICITE OU IMPLICITE D'AUCUNE SORTE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Les produits IBM sont garantis conformément aux dispositions des contrats au titre desquels ils sont fournis.

Chaque client est tenu de s'assurer qu'il respecte la réglementation applicable. IBM ne donne aucun avis juridique et ne garantit pas que ses services ou produits sont conformes aux lois applicables.

Déclaration de bonnes pratiques de sécurité : la sécurité du système IT englobe la protection des systèmes et des informations grâce à la prévention, la détection et la réponse en cas d'accès internes et externes non autorisés. Un accès non autorisé peut entraîner la modification, la destruction, le détournement ou l'utilisation impropre des informations, ou une détérioration ou une utilisation impropre de vos systèmes, notamment en vue de les utiliser pour attaquer autrui. Aucun système ou produit IT ne doit être considéré comme entièrement sécurisé, et aucun produit, service ou dispositif de sécurité ne peut être entièrement efficace pour empêcher une utilisation ou un accès inappropriés. Les systèmes, produits et services d'IBM sont conçus pour fonctionner dans le cadre d'une stratégie de sécurité globale et conforme à la loi qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent nécessiter des performances maximales des autres systèmes, produits et services. IBM NE GARANTIT PAS QUE LES SYSTÈMES, PRODUITS OU SERVICES SONT PROTÉGÉS CONTRE LES AGISSEMENTS MALVEILLANTS OU ILLÉGAUX D'UN TIERS OU QU'ILS PROTÉGERONT VOTRE ENTREPRISE CONTRE DE TELS AGISSEMENTS.

IBM