4 approches d'Azure Sentinel Les principaux problèmes de sécurité IT

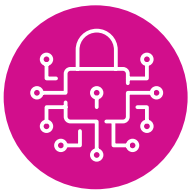
Maximisez les avantages et les capacités de votre investissement dans la sécurité.

Insight Microsoft

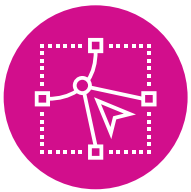
Étude du paysage des menaces

Il est essentiel de trouver la bonne combinaison d'outils, de technologies et de compétences pour assurer la réussite d'un Centre des opérations de sécurité (SOC). Cela est particulièrement vrai suite à l'augmentation récente du volume de cyberattaques. Maintenant, pensez que le coût moyen d'une violation causée par un ransomware en 2021 atteint le montant exceptionnel de 4,62 millions de dollars américains[1]. Cela représente beaucoup de dommages potentiels. Il n'est donc pas surprenant que les équipes de sécurité IT du monde entier soient soumises à une certaine pression pour améliorer le temps de réponse et éviter les pertes futures.

Pour lutter contre cette tendance en constante évolution, les entreprises devraient consacrer en moyenne 24,4 millions de dollars au budget de sécurité informatique en 2022.[2] Celles qui cherchent à héberger des données sur site et dans le Cloud devront réévaluer leurs solutions existantes pour assurer une couverture complète sur tous les sites opérationnels, bureaux à domicile, systèmes de communication et partout ailleurs.

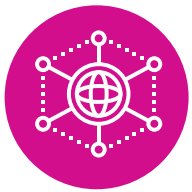


L'augmentation des terminaux et des volumes de données exige une sécurité évolutive.



Les solutions ponctuelles présentent une portée limitée et des défis d'intégration supplémentaires.

Il est devenu plus difficile de trouver et de retenir des talents en matière de sécurité.



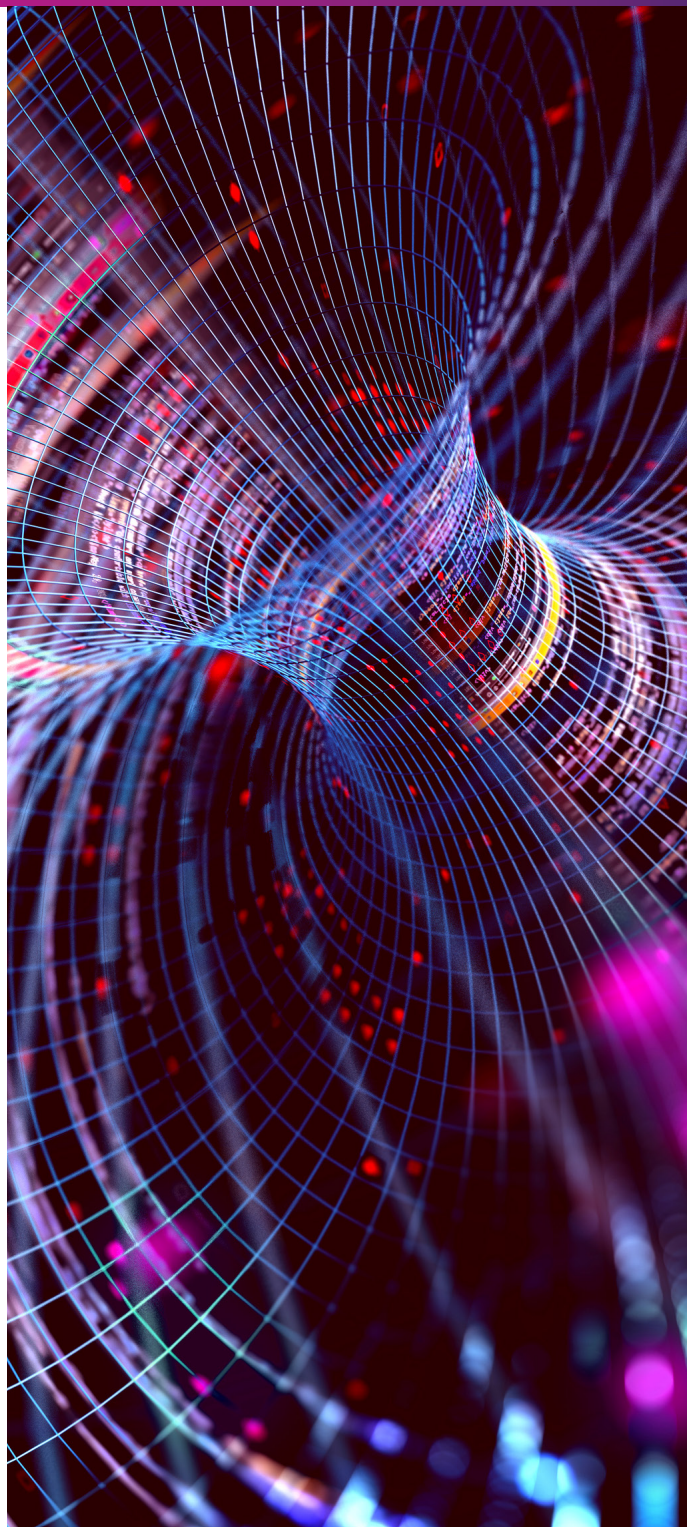
La complexité des environnements IT augmente sans cesse, avec d'innombrables vecteurs d'attaques.

Pensez à vos données, utilisateurs et systèmes.

Une visibilité totale est requise pour détecter et contrecarrer les dommages potentiels, ainsi que pour pouvoir exploiter plusieurs systèmes à partir d'un point de départ unique et prendre le contrôle de l'ensemble de l'environnement IT. Sachant qu'il faut en moyenne 280 jours aux entreprises pour détecter une violation, une quantité incalculable de données, d'enregistrements et de systèmes peut être compromise avant même que des mesures ne soient prises pour lutter contre l'intrusion. Une façon d'améliorer la visibilité et de réduire ce barrage consiste à mettre en œuvre la gestion des identités et des accès. Lorsqu'elles sont capables de suivre les tendances du comportement des utilisateurs pour découvrir des schémas, les entreprises peuvent réduire la fenêtre de remédiation et combler les lacunes qui passaient inaperçues auparavant.

Lors de la mise en œuvre de la gestion des identités et des accès, envisagez de poser les questions suivantes :

- Dans quelle mesure vos données sont-elles sensibles ?
- Qui a vraiment besoin d'accéder à des fichiers spécifiques ?
- Quand et pendant combien de temps l'accès est-il nécessaire ?
- Devez-vous mettre en place un programme de classification des données ?
- Avez-vous établi des types d'utilisateurs ?
- Quand avez-vous examiné les autorisations pour la dernière fois ?
- Comment vérifiez-vous les identités et les points d'accès ?
- Quelles alternatives avez-vous envisagées pour l'authentification ?
- La biométrie serait-elle un choix intéressant ?
- Avez-vous remarqué des lacunes ou des schémas flagrants ?
- Comment pourriez-vous faire évoluer votre approche actuelle vers une approche plus sécurisée ?



Les avantages d'un programme de sécurité moderne

Il peut être utile de noter que 89 % des entreprises ont déjà adopté, ou prévoient d'adopter, une approche multicloud.[4] Si votre entreprise fait partie de cette majorité, vous pouvez disposer d'un environnement IT diversifié. La capacité à traquer avec succès les données, les hackers et plus encore améliorera l'efficacité des efforts de prévention déployés par votre équipe de sécurité IT. Autre caractéristique clé d'un programme solide : une gouvernance complète qui traite de la propriété et de la responsabilité. En définissant des objectifs, des rôles et des processus de sécurité, les entreprises peuvent mieux organiser les directives et la formation, ainsi que valider les utilisateurs et les processus.

Autre considération à garder à l'esprit, 57 % des entreprises interrogées dans le rapport « The State of IT Modernisation 2020 » ont déclaré que la mise à niveau de l'infrastructure et des processus de sécurité était un obstacle majeur dans leur quête de modernisation de leurs environnements d'exploitation IT.[3] C'est là qu'un partenaire tiers peut être en mesure d'apporter une valeur ajoutée grâce aux services d'automatisation.

L'automatisation au sein du SOC offre :

- Des capacités de détection, de réponse et de remédiation plus rapides
- Moins d'erreurs et moins de « pression liée aux alertes »
- Des ressources de sécurité libérées des tâches répétitives
- Une amélioration de l'expérience et de la satisfaction utilisateur

Investir dans une solution SIEM native du Cloud

Microsoft® Azure Sentinel® est une solution native du Cloud native de SIEM (Security Information and Event Management) et de SOAR (Security Orchestration Automation and Response) fournie en tant que service Cloud. En tirant parti de la capacité de la solution à fournir des analyses de sécurité intelligentes pour l'ensemble de l'environnement, les entreprises peuvent arrêter les menaces avant qu'elles ne causent des dommages. Solution évolutive et permanente, Azure Sentinel renforcera ou remplacera vos outils de sécurité existants pour améliorer la visibilité sur votre paysage de menaces.

- Obtenez une vue d'ensemble de votre entreprise.
- Rationalisez la détection et la réponse grâce à l'intelligence artificielle (IA).
- Éliminez la configuration et la maintenance de l'infrastructure de sécurité.
- Évoluez pour répondre aux nouveaux besoins de sécurité.

En outre, cette solution réduit les coûts de 48 % et se déploie 67 % plus rapidement que les SIEM traditionnels.[5] Par conséquent, les entreprises peuvent consacrer plus de temps à la détection des menaces réelles, en mettant en place des opérations de sécurité plus stratégiques. Comment cela fonctionne-t-il exactement ? Comment la solution utilise-t-elle l'IA et l'apprentissage automatique pour détecter, analyser les menaces et mener l'enquête ? Nous aborderons le processus en quatre étapes à la page suivante.

4 étapes vers les opérations de sécurité de nouvelle génération

1. Collecter

Les entreprises hébergent aujourd'hui des documents, des données, des enregistrements et plus encore sur une multitude d'appareils, d'applications et d'infrastructures, à la fois sur site et dans plusieurs Clouds. De plus, tous ces fichiers sensibles sont accessibles par les utilisateurs à tout moment, où qu'ils se trouvent. Azure Sentinel® collecte des données à l'échelle du Cloud, agrégeant l'infrastructure et les dispositifs de sécurité tels que les pare-feu.

2. Détecter

Trouver des occurrences régulières et des schémas de cyberattaques peut aider les entreprises à bloquer les menaces. L'analyse et la veille inégalée sur les menaces aident même les entreprises à découvrir des menaces jusqu'alors indétectables et à minimiser les risques de faux positifs. Imaginez que vous puissiez surveiller et corréler des millions d'anomalies à la fois, puis tirer rapidement de la valeur du rapport. C'est ce qu'offre cette solution.

3. Investiguer

Tirant parti des décennies d'expérience en cybersécurité de Microsoft, Azure Sentinel chasse les activités suspectes à grande échelle avec les conseils de l'IA, éliminant ainsi le besoin de matériel ou de machines virtuelles. La solution apprend, à partir des logs quotidiens, à réduire le bruit, afin que les équipes de sécurité puissent se concentrer sur les signaux essentiels.

4. Répondre

Grâce à l'orchestration intégrée et à l'automatisation des tâches courantes, les entreprises peuvent réagir rapidement aux incidents. En tirant parti de la technologie intelligente, votre équipe de sécurité IT gagnera du temps tout en améliorant la précision. Par exemple, les playbooks déclenchés par des règles d'analyse ou d'automatisation peuvent être exécutés dans Azure Sentinel pour rationaliser le temps de réponse et bloquer les acteurs malveillants.

Pourquoi Insight pour Azure Sentinel ?

Chez Insight, nous estimons que le moment est idéal pour améliorer votre posture de sécurité, en particulier avec l'essor du télétravail et du travail hybride. Appuyez-vous sur nos années d'expérience pour protéger votre entreprise contre les cybermenaces en constante évolution. Ensemble, nous aiderons votre entreprise à obtenir une solution flexible et évolutive, tirant parti de capacités d'IA et d'apprentissage automatique de pointe. L'objectif : améliorer la sécurité, la visibilité et le contrôle de l'ensemble de votre environnement IT.

Nous sommes l'un des principaux partenaires Microsoft et l'un des 12 partenaires mentionnés publiquement par Microsoft pour la consultation et l'apport de services Azure Sentinel® :

- 18 compétences Microsoft Gold et Silver
- Plus de 25 ans de partenariat avec Microsoft
- Plus de 1000 ingénieurs et professionnels du service axés sur Azure
- Expert Managed Services Provider (MSP) Azure et plus grand partenaire Azure
- Lauréat du prix Microsoft Security 20/20 pour la catégorie Partenaire de déploiement Azure Security de l'année
- Support tout au long de la prestation des services de conseil

À propos d'Insight

Insight Enterprises, Inc. est un intégrateur de solutions Fortune 500 qui compte 11 500 collaborateurs dans le monde, aidant les organisations à accélérer leur parcours numérique pour moderniser leur entreprise et maximiser la valeur de la technologie. Nous permettons une transformation sécurisée de bout en bout et répondons aux besoins de nos clients grâce à un portefeuille complet de solutions, à des partenariats de grande envergure et à plus de 33 ans d'expertise IT étendue. Nommés meilleur employeur au monde par Forbes et certifiés Great Place to Work, nous amplifions nos solutions et services grâce à une échelle mondiale, à une expertise locale et à une expérience de classe mondiale dans l'e-commerce, et ne manquons pas la moindre occasion de concrétiser les ambitions numériques de nos clients.

Insight®

fr.insight.com

Sources :

[1] IBM Security. (2021). Cost of a Data Breach Report.

[2] Channel Futures. (Février 2022). The High Cost of Ransomware.

[3] Insight. The State of IT Modernisation 2020.

[4] Flexera. (Mars 2022). 2022 State of the Cloud Report.

[5] Forrester. (Novembre 2020). The Total Economic Impact™ of Microsoft Azure Sentinel. Cost Savings and Business Benefits Enabled By Azure Sentinel.

MKT6231