Insight®

Relever les principaux défis des environnements de sécurité multi-fournisseurs

Guide pour surmonter le burnout lié à la sécurité et renforcer vos défenses avec Insight et Microsoft Sentinel

Une sécurité sous tension

des répondants à l'enquête 2020 CISCO Benchmark Survey de Cisco, auprès des RSSI, déclarent souffrir d'un épuisement lié à la cybersécurité (ce qui se traduit par un quasi-abandon de leur défense proactive contre les acteurs malveillants).

Parmi les personnes qui en souffrent, **93 % reçoivent plus de**

5000 **alertes par jour.**

Cela montre que la complexité semble être l'une des principales causes de burnout lié à la sécurité.[1]

Pour gérer un environnement de menace complexe, la plupart des organisations utilisent plusieurs solutions de sécurité. Mais, en plus d'être difficiles, la gestion et l'orchestration des alertes provenant de plusieurs sources disparates exposent également les organisations à plus de risques.

Une surabondance d'alertes signifie qu'il peut simplement y en avoir trop à traiter. Cela exerce un impact sur la connaissance de la situation et la visibilité dont bénéficie l'équipe, et peut potentiellement exposer l'entreprise à des menaces plus importantes et plus préjudiciables au fil du temps.

Selon Fady Younes, directeur de la cybersécurité chez Cisco : « L'incapacité à intégrer plusieurs solutions de sécurité peut également créer des fossés dans la couverture ou générer une situation dans laquelle l'équipe IT ne comprend pas correctement la protection qu'offre une solution particulière, ou son fonctionnement. Cela exerce un impact sur la visibilité et la connaissance de l'état de sécurité réel du réseau. »[2]

Il est plus difficile de déterminer quels risques et alertes doivent être priorisés dans ces environnements.

Toutes les alertes n'ont pas la même gravité, et les meilleures stratégies de sécurité adaptent les contrôles de sécurité et allouent les ressources en fonction du niveau de risque.

Dans des environnements multicloud diversifiés, la reprise après sinistre devient incroyablement complexe, et nécessite donc une culture de sécurité proactive plutôt que réactive.

« Gérer les problèmes d'intégration et un volume élevé d'alertes de sécurité peut empêcher les ingénieurs de sécurité de relever d'autres défis auxquels ils sont également confrontés... »

- Fady Younes, Directeur de la cybersécurité, Moyen-Orient et Afrique chez Cisco

SIEM et SOAR

Les équipes de sécurité ont deux objectifs principaux : savoir ce qui se passe dans leur environnement IT et répondre à ces informations. Les solutions SIEM (Security Information and Event Management) et SOAR (Security Orchestration, Automation, and Response) permettent d'atteindre ces objectifs.

Les outils SIEM rassemblent et agrègent les données d'événements provenant de diverses sources au sein d'un environnement IT, puis analysent et classent les événements par ordre de priorité ou de criticité. Les équipes de sécurité assument la responsabilité de la recherche et de la réponse aux menaces, ainsi que de la correction de la plateforme SIEM.

Les outils SOAR fournissent une analyse et une automatisation avancées qui s'appuient sur les capacités des outils SIEM, pour une réponse plus autonome aux menaces. Les outils SOAR exploitent autant de données en temps réel que possible et dépendent de la compétence des responsables. Ces outils sont plus ou moins efficaces en fonction de la manière dont ils sont utilisés.

déclarent que SOAR est très ou extrêmement important pour la posture de sécurité globale de leur organisation.

Cas d'utilisation pour SOAR :

- 65 % Triage SIEM
- 62 % Attaques par hameçonnage
- 62 % Renseignements sur les menaces

Résultats des déploiements de SOAR :

- Résolution des incidents plus rapide
- Amélioration de l'efficacité du personnel
- Coûts globaux réduits[3]

Qu’est-ce qui distingue Microsoft Sentinel ?

Le SOAR est la fonctionnalité de Sentinel qui la différencie de ses concurrents. Il permet aux équipes de sécurité d’écrire du code ou des playbooks dans Sentinel pour répondre automatiquement aux menaces lorsqu’elles arrivent. Cela permet à l’équipe du SOC de réduire la fatigue liée aux alertes et à se concentrer sur les éléments essentiels.

Nos clients apprécient fortement de pouvoir corréler les alertes et les incidents ; en dessinant une carte de chaque incident associé à une entité spécifique. Ce que je montre aux clients lors d’une démonstration, en général, c’est un scénario où un attaquant aléatoire a réussi à accéder à l’environnement, à augmenter ses privilèges, à effectuer un téléchargement en masse de données commerciales, puis à supprimer son compte. Voilà quatre alertes distinctes que vous recevriez dans n’importe quel SOAR ou SIEM. Mais dans Microsoft Sentinel, vous pouvez voir un graphique d’une entité avec quatre lignes différentes pour chaque alerte générée, ainsi qu’une chronologie de ces événements. Microsoft Sentinel facilite vraiment la chasse aux menaces. »

— Consultant associé, InfoSec, Insight

Le cas de Microsoft Sentinel

Microsoft Sentinel™ associe la puissance SIEM et SOAR en une seule solution. Si vous avez déjà investi dans Microsoft® Sentinel, vous êtes sur la voie d’une sécurité renforcée.

La plateforme Sentinel peut vous aider à :

identifier les menaces avant qu’elles n’affectent votre entreprise;

répondre rapidement et avec plus de précision;

simplifier la sécurité dans les environnements hybrides, multicloud, sans serveur et autres environnements modernes;

réduire les coûts par rapport aux anciennes solutions SIEM pour investiguer sur les menaces, le licensing, le stockage, l’infrastructure, la gestion et le déploiement.

L’outil s’appuie sur l’expérience approfondie de Microsoft en matière de sécurité et sur les dernières capacités d’intelligence artificielle, et fonctionne en harmonie avec d’autres produits Microsoft. Il est rapide à configurer et facile à mettre à l’échelle.

Un hub, de nombreux points de données

Les environnements de solutions multifournisseurs deviennent moins complexes à gérer avec Microsoft Sentinel. La capacité de Sentinel à extraire des sources de données de l’ensemble de l’écosystème de solutions de sécurité multifournisseurs offre visibilité et contrôle aux organisations, pour simplifier la chasse aux menaces, réduire la pression liée aux alertes et capturer une image fidèle de votre posture de sécurité.

Meilleures pratiques de mise en œuvre

Les premiers pas avec Microsoft Sentinel sont relativement simples. Avant la mise en œuvre, nous conseillons d'établir une gouvernance et des politiques claires. Les considérations comprennent les normes de conformité, les exigences de coût, les plans de stockage, la reprise après sinistre, le personnel de l'équipe de sécurité et les plans d'intervention en cas d'incident.

Jour 1 :

Activez Microsoft Sentinel.

Connectez les sources de données.

Commencez à créer des requêtes pour enquêter sur les données.

Comme de nombreux autres outils de SIEM, Syslog et CEF servent de points d'ingestion. Vous pouvez utiliser n'importe quelle distribution Linux® de votre choix, y compris la distribution Linux de Microsoft, et installer les redirecteurs CEF et Syslog pour transférer les logs à Microsoft Sentinel qui pourra les ingérer.

Microsoft a également conçu Sentinel pour prendre en charge les logs de formatage génériques dans un format commun, afin que même les logs provenant d'appareils existants ou spécialisés puissent être intégrés et analysés.

Assurer une sécurité globale.

Microsoft Sentinel offre le maximum de son efficacité dans le cadre d'une approche programmatique plus étendue de la cybersécurité. Assurez-vous que votre organisation utilise les meilleures pratiques sur l'ensemble du spectre de la cybersécurité : Identifier, Protéger, Détecter, Répondre et Récupérer.

SOLUTION INSIGHT

Atténuez les risques et protégez votre organisation.

Insight dispose d'une solide pratique de sécurité et de l'impulsion nécessaire dans le contexte de la sécurité IT. Nous aidons les organisations à sécuriser leurs données et leurs réseaux depuis plus de 30 ans. En tant que groupe de conseillers, de fournisseurs de solutions et de spécialistes techniques, nous préservons la certification et l'immersion dans les dernières technologies de sécurité et les meilleures pratiques.

Jour 2 et + :

La flexibilité et le dynamisme de la plateforme seront évidents à ce stade. Voici plusieurs façons de maximiser considérablement les avantages de Microsoft Sentinel pour les besoins spécifiques et le profil de risque de votre organisation.

1.

Vérifiez vos transitaires de logs.

Si vous ne prêtez pas particulièrement attention à la santé de vos transitaires de logs et à la capacité de votre VAR, la situation peut rapidement se dégrader et l'ingestion de logs cessera. Lorsque les consultants Insight effectuent le déploiement de Microsoft Sentinel, nous utilisons des distributions Linux avec une partition pour le point de montage du log VAR séparé du système d'exploitation. Ainsi, si le répertoire se remplit, l'impact sur le système d'exploitation est moindre.

2.

Examinez vos taux d'ingestion.

Il est difficile d'estimer le nombre de logs que vous pouvez ingérer dès le début, mais après un mois ou deux, vous disposerez de suffisamment de données historiques pour prendre de meilleures décisions concernant le taux d'ingestion de données. Cela vous aidera à obtenir une meilleure rentabilité.

3.

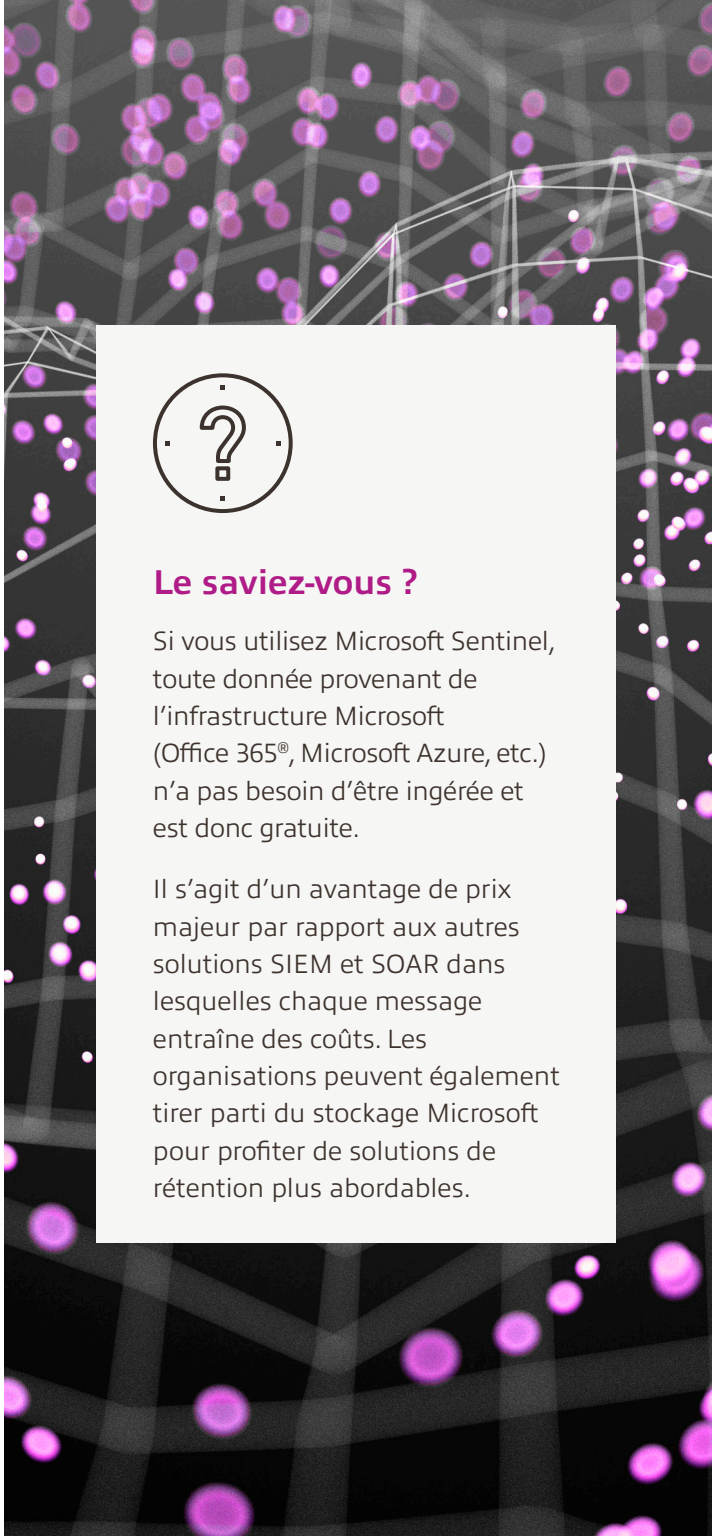
Minimisez les faux positifs.

De nombreuses règles prêtes à l'emploi, qui rendent compte des fonctions administratives à l'aide de l'analyse du comportement, peuvent générer des faux positifs. Microsoft a publié une fonctionnalité Sentinel appelée Watchlist pour aider à réduire ces faux positifs, le bruit qui en résulte et la pression des alertes. La liste de surveillance vous permet d'intégrer des requêtes (ou CSV d'attributs différents) dans des règles analytiques qui examinent une liste de surveillance ou une paire d'identifiants clés. Elle ne déclenche pas d'alerte sur des activités spécifiques.

4.

Utilisez un tenant centralisé.

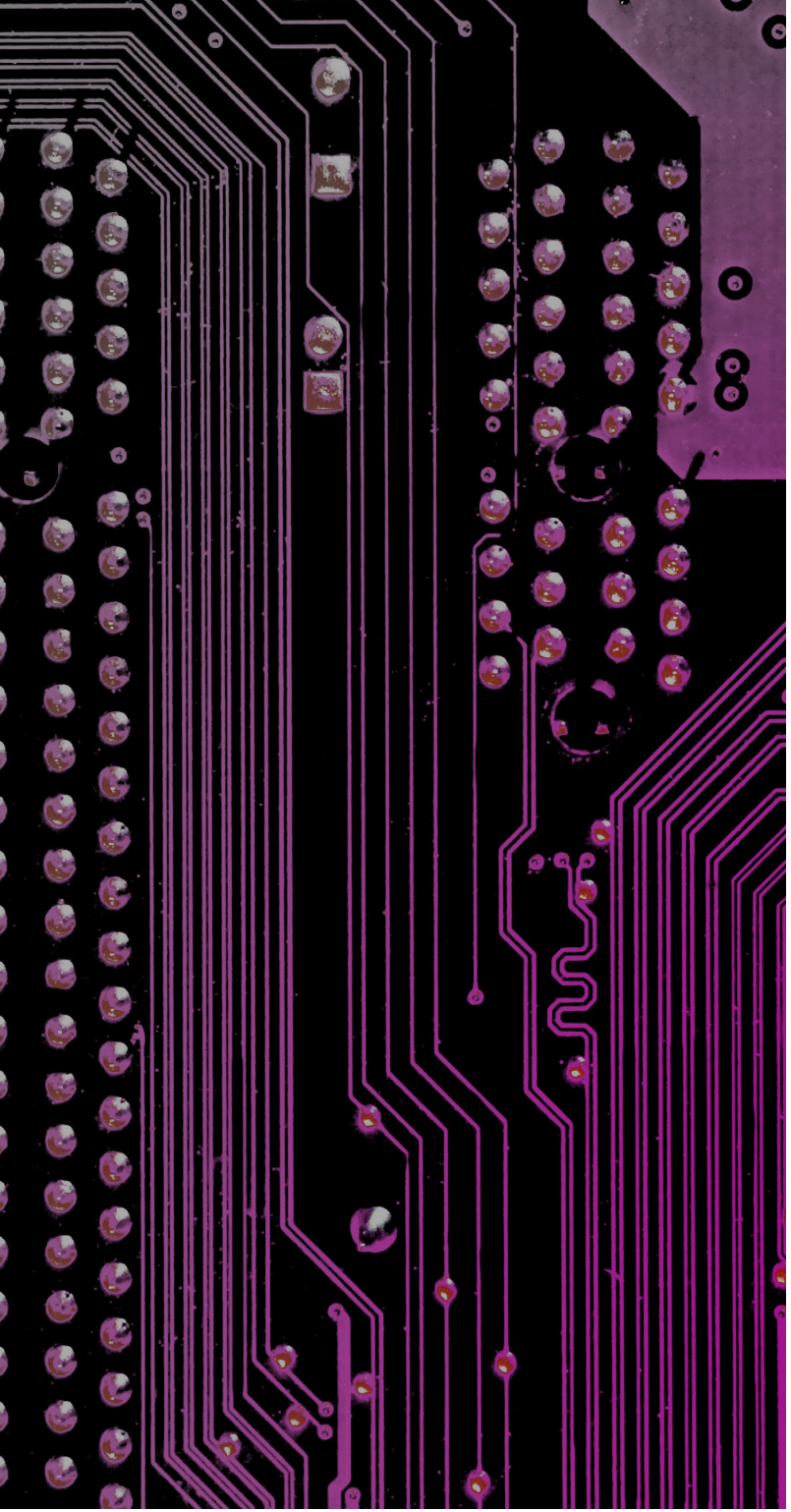
Si vous surveillez différents tenants Azure®, vous devez créer différents espaces de travail d'analyse de journaux et différentes installations Microsoft Sentinel dans chacun de ces locataires. En utilisant Azure Lighthouse pour surveiller ces espaces de travail dans un tenant centralisé, vous pouvez affiner les règles analytiques, accéder à la source d'informations fiables et déployer des règles pour tous les tenants. Cela vous aidera à établir une référence cohérente pour les seuils, la fréquence d'exécution et d'autres paramètres.



Le saviez-vous ?

Si vous utilisez Microsoft Sentinel, toute donnée provenant de l'infrastructure Microsoft (Office 365®, Microsoft Azure, etc.) n'a pas besoin d'être ingérée et est donc gratuite.

Il s'agit d'un avantage de prix majeur par rapport aux autres solutions SIEM et SOAR dans lesquelles chaque message entraîne des coûts. Les organisations peuvent également tirer parti du stockage Microsoft pour profiter de solutions de rétention plus abordables.



5.

Effectuez un réglage prêt à l'emploi.

Microsoft Sentinel offre l'avantage d'une intégration fluide à votre écosystème Microsoft. Nos consultants conseillent régulièrement aux clients d'utiliser Microsoft Defender for Identity (MDI) pour Active Directory® (AD) sur site, par exemple. Cependant, lorsque vous intégrez MDI à Sentinel, le paramètre par défaut transmet automatiquement toutes les alertes provenant de MDI. Vous pouvez accéder au connecteur plug-in et le régler pour ne pas être alerté sur des informations non urgentes, afin de recevoir uniquement les alertes d'une plage de gravité spécifiée.

Examinez également les gravités des règles analytiques existantes et faites-les remonter, décroître ou supprimez-les, en fonction de vos besoins. De nombreuses règles analytiques prêtes à l'emploi s'exécutent à une fréquence définie qui peut être trop importante. Nous vous conseillons d'utiliser des règles analytiques toutes les 15 ou 30 minutes pour les alertes de haute importance, et de les exécuter une seule fois par jour pour les alertes de faible importance ou d'information qui n'ont pas beaucoup d'impact sur l'entreprise. En fin de compte, le réglage vous aidera à minimiser la pression et le bruit liés aux alertes.

6.

Évaluez la parité.

Qu'utilisiez-vous pour sécuriser votre environnement IT avant Microsoft Sentinel ? Quelles sont les similitudes et les différences ? Nos consultants vous suggèrent de comparer votre ancien système et l'environnement Microsoft Sentinel pour étudier les résultats, les tableaux de bord, les alertes, les sources des logs et d'autres attributs clés pour assurer la parité. Aucune source de données ne doit être oubliée. Cela vous aide également à vous assurer que vous comprenez parfaitement la nouvelle portée des tâches quotidiennes, des soins et de l'alimentation, ainsi que les exigences en matière de personnel pour la prise en charge de la nouvelle plateforme.

7.

Consultez les conseils de Microsoft.

Microsoft a publié des recommandations d'activités régulières à effectuer afin de garantir que Sentinel vous offre la meilleure sécurité possible. Examinez-les pour obtenir des suggestions sur les tâches quotidiennes, hebdomadaires et mensuelles, les intégrations à configurer et les processus de gestion et de réponse aux incidents.

Opportunités d'automatisation

L'un des atouts de la plateforme Sentinel de Microsoft réside dans ses capacités d'automatisation. Tirez parti de l'automatisation pour obtenir une efficacité et une sécurité optimales.

Voici quelques façons d'automatiser avec Sentinel :

Rétention

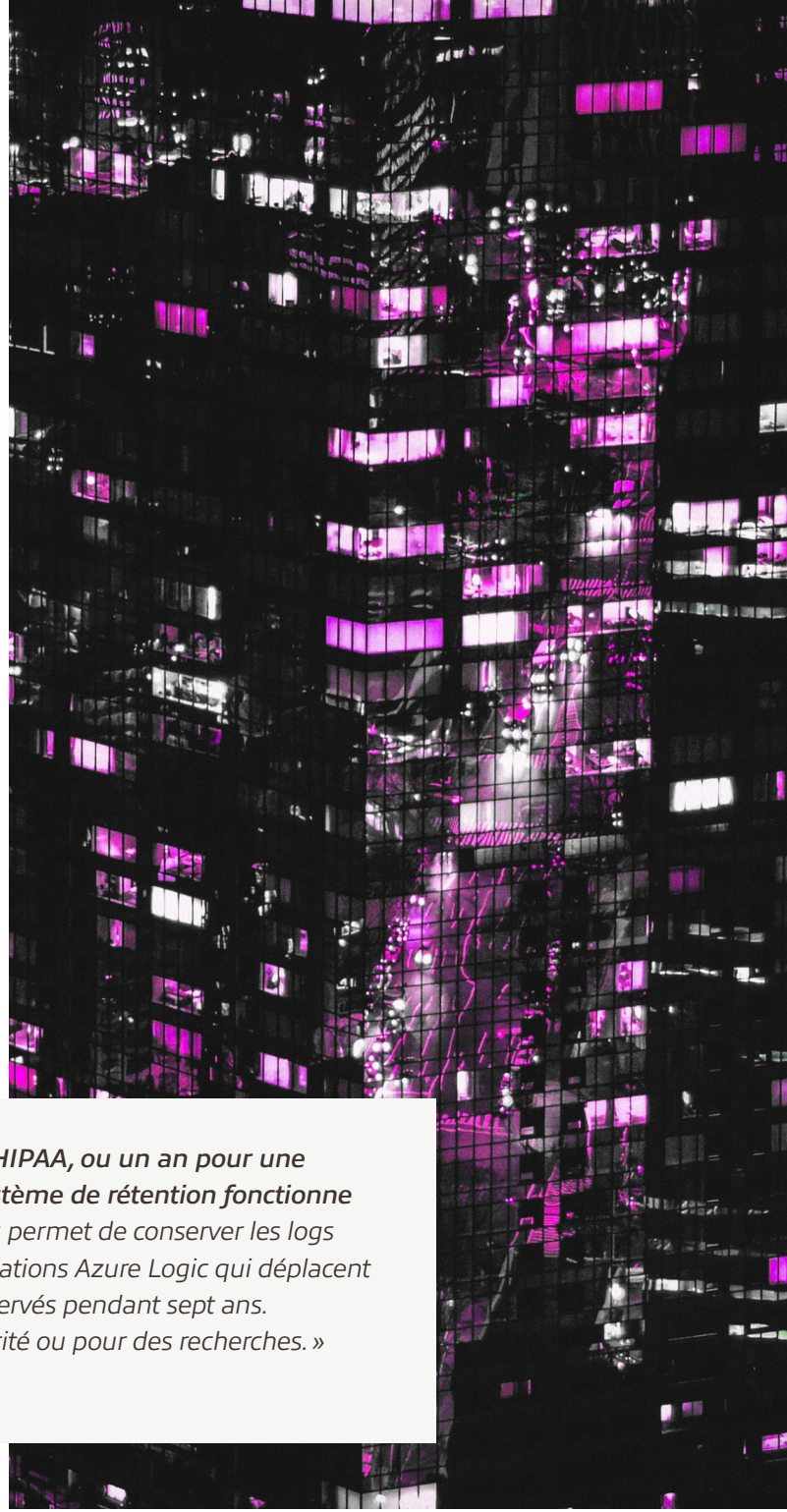
Chaque organisation a des besoins différents en matière de conservation des données, selon les exigences du secteur et les exigences légales et de conformité. Microsoft Sentinel offre la possibilité d'automatiser le stockage pendant des périodes définies. Votre équipe sait donc que ce point est traité, sans avoir à définir de rappels ni à se soucier de la capacité.

Playbooks

Pour les automatisations plus complexes, les playbooks sont une excellente option. Les playbooks dans Microsoft Sentinel peuvent être configurés pour différentes tâches, telles que :

- blocage d'un utilisateur après une alerte d'échec de connexion
- création d'un incident ServiceNow® qui alimente votre système de tickets
- modification de la CMDB dans ServiceNow en cas de modification des appareils bloqués sur le réseau

GitHub, appartenant à Microsoft, héberge de nombreux playbooks et idées de personnalisation, ainsi que des automatisations spécifiques aux fournisseurs à explorer dans Microsoft Sentinel.



> ***Imaginons que certains clients demandent sept ans de conservation des données pour l'HIPAA, ou un an pour une conformité réglementaire gouvernementale ou NIST. Il est difficile de déterminer quel système de rétention fonctionne le mieux pour une organisation.*** *Le stockage Blob de Microsoft est une bonne option : il vous permet de conserver les logs de manière rentable pendant sept ou huit ans. Pour simplifier ce point, nous créons des applications Azure Logic qui déplacent automatiquement les logs ingérés de Microsoft Sentinel vers le stockage Blob, où ils sont conservés pendant sept ans. Les organisations ont toujours accès aux logs si elles en ont besoin pour une enquête de sécurité ou pour des recherches. »*
>
> **— Consultant associé, InfoSec, Insight**

Tourner le regard vers l'avenir

Il existe d'innombrables façons d'étendre et d'améliorer Microsoft Sentinel. Les opportunités continuent de croître à mesure que la plateforme et la communauté d'utilisateurs mûrissent.

BYO ML

Le Bring Your Own Machine Learning (BYO ML) est un domaine qui attire beaucoup l'attention. Cette page Microsoft GitHub sert de référentiel pour les dernières informations, avec une bibliothèque croissante d'exemples de notebooks de formation. Les organisations utilisent le BYO ML pour lancer Databricks et proposer des formations et des analyses via un environnement Spark, en extrayant toutes les données de Sentinel, en créant des modèles d'accès à distance ou de comportement anormal, etc.

> ***Vous n'aurez pas besoin d'un doctorat pour y parvenir.*** *Une grande partie de la formation et des modèles communautaires offrent une assez bonne approximation, qui doit simplement être personnalisée pour votre environnement. D'autres SIEM proposent des éléments similaires, mais je trouve qu'il est assez intéressant de savoir que vous pouvez bénéficier d'une expérience très native de la science des données : vous avez un notebook Jupyter, différentes bibliothèques de science des données Python, et vous extrayez des données directement de l'environnement où le notebook est exécuté. »*
>
> **- Architecte principal (cybersécurité, réseau, science des données), Insight**

Visualisation avancée

Les workbooks Azure Monitor de Microsoft Sentinel offrent une visualisation riche des données. Bien sûr, ce point est extrêmement utile pour les équipes de sécurité. La consultation des données peut faciliter l'identification des points faibles et des vulnérabilités, aidant ainsi les équipes de sécurité à établir des priorités. La visualisation peut également aider les équipes de sécurité à justifier les budgets auprès de la direction, avec un impact rapide. À l'avenir, nous pensons que la visualisation des données sera un objectif clé ; les communautés d'utilisateurs vont développer des workbooks personnalisés pour répondre à tout besoin de sécurité ou de l'entreprise.

SOLUTION INSIGHT

Nos consultants en services de sécurité peuvent vous aider à examiner les implications de vos activités d'entreprise en matière de sécurité et à adopter des solutions adaptées à vos besoins et à vos objectifs. Nous commençons par évaluer votre environnement actuel, vos défis et vos exigences.

Services managés

En raison du manque de temps et de ressources, aujourd'hui, les organisations ne peuvent remédier

50 % qu'aux menaces de sécurité légitimes.[1]

De nombreuses organisations ont du mal à attirer et à retenir des professionnels de la sécurité expérimentés, qui connaissent les ensembles d'outils les plus récents en SIEM, SOAR et Security Operations Center (SOC). Nous constatons déjà une consolidation globale des talents en sécurité dans les organisations de services qui peuvent gérer efficacement les environnements de sécurité, ainsi que fournir un support critique concernant la préparation aux ransomwares, l'architecture de la sécurité, la réponse aux incidents et la remédiation.

Dans de nombreux cas, la gestion du temps est le principal défi. L'apprentissage des moyens d'accroître l'automatisation ou de tirer parti de l'apprentissage automatique pour améliorer la chasse aux menaces peut être éclipsé par les innombrables exigences quotidiennes de la gestion d'une équipe de sécurité.

Le secret pour renforcer votre sécurité ? Les services managés.

Insight propose des services de sécurité managés (MSS, Managed Security Services) qui s'appuient sur les capacités de Microsoft Sentinel et fournissent une surveillance de votre environnement 24/7. En associant les meilleures pratiques renforcées de l'industrie avec des techniques de pointe pour la réduction des risques, nous aidons les clients à alléger le lourd fardeau lié à la prise en charge et à l'amélioration d'un environnement de sécurité dynamique.

Une approche avancée

Nos consultants en services de sécurité peuvent vous aider à examiner les implications de vos activités d'entreprise en matière de sécurité et à adopter des solutions adaptées à vos besoins et à vos objectifs. Nous commençons par évaluer votre environnement actuel, vos défis et vos exigences.

16 ans
d'expérience dans la gestion des incidents et des menaces

Plus de 1500
architectes, ingénieurs et experts, et prestation de services

Résultats liés à la sécurité managée :


temps de réponse plus rapides


gouvernance et conformité renforcées


contexte et visibilité plus riches


détection améliorée des menaces


réduction du fardeau pour l'équipe de sécurité

Oubliez vos limites

Microsoft Sentinel est facile à mettre en œuvre, mais nécessite des compétences supplémentaires pour une optimisation correcte.

Heureusement, il existe peu de limites quant à la sécurité complète que la plateforme peut vous apporter. Avec une équipe de confiance comme Insight, il est plus facile que jamais de découvrir la valeur de votre investissement. Nos consultants, techniciens et architectes possèdent une expertise de pointe avec Microsoft Sentinel, dans un large éventail d'environnements clients.

Où que vous en soyez dans votre parcours Sentinel, vous pouvez utiliser Insight pour bénéficier :

- d'une évaluation de votre environnement de sécurité actuel
- d'une évaluation de la préparation à Microsoft Sentinel
- de déploiement, d'intégration et de personnalisation de Microsoft Sentinel
- de services de sécurité managés pour gérer Microsoft Sentinel
- d'optimnisation de Microsoft Sentinel, d'automatisations et d'un réglage avancé des fonctionnalités

Contactez notre équipe aujourd'hui même pour discuter de vos besoins

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.

Pour en savoir plus, rendez-vous sur :
https://fr.insight.com/fr_FR/home.html

Insight®

Sources :
[1] Cisco. 2020. Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020. CISO Benchmark Survey.
[2] Younes, F. (21 jan. 2021). Complexity Still Remains Cybersecurity Worst Enemy. Techeconomy.ng.
[3] Rockett, J. (25 juin 2020). 2020 SOAR Report Highlights Key Drivers and Impacts. Swimlane.