Démarrage rapide de Microsoft Sentinel

Bénéficiez d'une vue d'ensemble de votre entreprise grâce au SIEM pour un monde moderne.

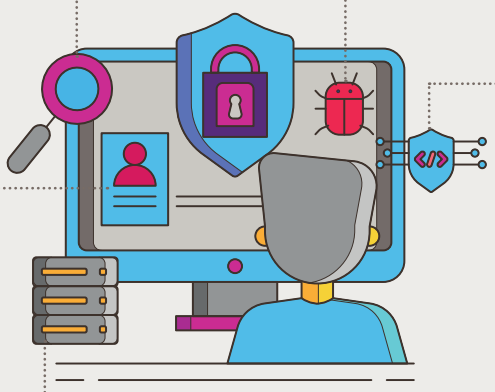
Vue globale de la solution

Contexte et défi pour les entreprises

À mesure que l'IT devient plus stratégique, l'importance de la sécurité augmente au quotidien. Les Solutions de gestion des événements et des informations de sécurité (Security information and event management, SIEM) conçues pour les environnements d'hier peinent à suivre le rythme des défis d'aujourd'hui, sans parler des risques inimaginables de demain.

L'enquête est complexe et chronophage
Chaque seconde compte lorsque le personnel SecOps gère une menace qui pourrait mettre en danger leur organisation. L'horloge tourne rapidement, mais l'enquête nécessite des analystes de sécurité hautement qualifiés et peut souvent prendre des jours ou des semaines.

Les menaces continuent de croître en complexité et en volume
Les attaques sont de plus en plus hétérogènes. Une attaque caractéristique couvre différentes parties de l'entreprise et traverse différents types de ressources : elle peut commencer à partir d'un appareil IdO (Internet of things, IoT), passer à un terminal, se propager à un service Cloud ou à une base de données, impliquer plusieurs comptes utilisateur ou locataires, etc.



Il existe une pénurie mondiale d'analystes et d'expériences en matière de sécurité.
Le besoin de professionnels qualifiés en matière de sécurité a considérablement augmenté, et l'offre ne peut pas répondre à la demande actuelle ou future.

Fatigue d'alerte : Les centres d'opérations de sécurité (Security Operation Centres, SOC) voient trop d'alertes provenant de produits déconnectés
Les SOC ont généralement des dizaines de produits de sécurité, chacun produisant un grand volume d'alertes. Ces produits, pris isolément, présentent souvent des taux élevés de faux positifs et une mauvaise hiérarchisation des réponses, ce qui entraîne un bruit d'alerte sourd. Les attaques passent à travers les mailles du filet malgré la génération d'alertes. Malheureusement, les SIEM hérités ne fonctionnent qu'en tant qu'agrégateurs et n'augmentent pas les capacités de réponse. Les SOC ont besoin d'un moyen d'intégrer leurs produits de sécurité pour réduire le bruit, hiérarchiser les alertes et permettre l'investigation et la recherche dans l'ensemble des données.

Les solutions actuelles ne sont pas conçues pour les demandes d'aujourd'hui ou de demain
les SIEM sur site hérités nécessitent un matériel informatique puissant et une maintenance important qui les rendent coûteux à exploiter. Les besoins de stockage et de calcul augmentent considérablement lors d'un incident, ce qui est difficile à gérer pour une empreinte sur site. Le passage au Cloud a permis un nouveau degré d'évolutivité pour les entreprises, et avec l'explosion des données provenant du Cloud, les SIEM hérités sont de moins en moins capables de faire face à la demande.

C'est pourquoi Microsoft a développé Azure Sentinel, une solution SIEM entièrement native du Cloud.

Notre solution

Le service Microsoft Sentinel Quickstart fournit une implémentation à prix fixe et à portée fixe de la plateforme Microsoft Sentinel SIEM/SOAR (Security Orchestration, Automation, and Response). Il est conçu pour fournir la configuration initiale de la plateforme, l'espace de travail d'analyse des journaux prérequis et un ensemble de connecteurs de données par défaut pour introduire un ensemble de base de sources de journaux Microsoft. Il est également possible d'introduire d'autres sources de journaux, mais cela serait soumis à des coûts supplémentaires.

À la fin de ce module, le client disposera d'une plateforme Sentinel configurée sur laquelle il pourra exécuter sa propre fonction d'analyse de sécurité.

Résultats pour l'entreprise

Détectez et bloquez les menaces avant qu'elles ne causent des dommages avec Insight Microsoft Sentinel Quickstart.

Azure Sentinel offre des analyses de sécurité intelligentes et des renseignements sur les menaces dans toute l'entreprise, apportant une solution unique pour la détection des alertes, la visibilité des menaces, la recherche proactive et la réponse aux menaces.

Déploiement rapide et rentable

- Être opérationnel en un jour avec un ensemble initial de journaux.
- Pas besoin de commander du matériel informatique ou de payer pour des missions de conseil longues

Concentrez-vous sur la sécurité, soulagez les SecOps des tâches informatiques :

- Aucune configuration ou maintenance de l'infrastructure
- Service SIEM disponible dans le portail Azure
- Évoluez automatiquement, sans limite de ressources de calcul ou de stockage.
- Répondez rapidement grâce à l'automatisation et l'orchestration intégrées

Réduisez les coûts de sécurité et IT grâce à une solution SIEM économique :

- Aucun coût d'infrastructure, payez uniquement pour ce que vous utilisez
- Apportez vos données Office 365 gratuitement
- Facturation prévisible avec réservations de capacité
- Modèle flexible, aucun engagement annuel

Collectez des données de sécurité à l'échelle du Cloud à partir de toutes les sources de votre entreprise :

- Intégration pré-câblée avec les solutions Microsoft
- Connecteurs pour de nombreuses solutions partenaires Microsoft
- Prise en charge du format de journal standard pour toutes les sources

Détectez les menaces et analysez rapidement les données de sécurité grâce à l'IA :

- Des modèles d'apprentissage machine (Machine Learning, ML) basés sur des décennies d'expérience et d'apprentissage en sécurité de Microsoft et sur vos propres renseignements sur les menaces.
- Des millions de signaux filtrés en quelques incidents corrélés et hiérarchisés.
- Obtenez des alertes hiérarchisées et des conseils d'experts/spécialistes automatisés
- Visualisez l'attaque dans son ensemble et son impact
- Recherchez les activités suspectes à l'aide de requêtes prédéfinies et de bloc-notes Azure.

Notre partenaire Microsoft

Services associés

- Service de détection et de réponse managés
- Programme de sensibilisation à la sécurité
- Service d'appareil managé

Pourquoi Insight ?

Aujourd'hui, la technologie ne fait pas que soutenir l'entreprise : elle en devient l'essence même. Chez Insight, nous vous aidons à relever des défis complexes pour développer de nouvelles solutions et de nouveaux processus. Nous vous aiderons à gérer les priorités d'aujourd'hui et à vous préparer aux besoins de demain.

Portée et couverture internationales	Excellence opérationnelle et systèmes	ADN du logiciel	Solutions de services	Transformation de centres de données	Compétences techniques de nouvelle génération	Expertise en développement d'application et en IoT : Internet des objets	Insight Digital Workspace™	Alignement des partenaires

Pour plus d'informations, veuillez contacter votre gestionnaire de compte Insight.

+33 (0)1 30 67 25 00 | fr.insight.com

Insight