Solutions SIEM : cinq impératifs pour résoudre les grands défis des entreprises d'aujourd'hui

Après plus de dix années d'utilisation dans les environnements de production, les solutions de gestion des événements et des informations (SIEM) sont aujourd'hui considérées comme matures. La plupart d'entre elles mettent en œuvre les fonctionnalités essentielles que sont la collecte d'événements, leur corrélation, la génération d'alertes et la démonstration de la conformité aux exigences réglementaires. Mais le monde des entreprises connaît aujourd'hui de profonds changements. Les entreprises sont confrontées à de nouvelles menaces telles que les attaques ciblées et persistantes, à de nouvelles tendances comme la mobilité, le cloud et la virtualisation, ainsi qu'à une réorientation des priorités commerciales vers l'acquisition de nouveaux clients, l'efficacité opérationnelle et la réduction des coûts. En conséquence, les solutions SIEM doivent se doter de fonctionnalités plus évoluées pour résoudre des défis plus importants.

McAfee a interrogé les utilisateurs de solutions SIEM sur les principaux problèmes rencontrés avec ces dernières. Ils sont au nombre de cinq :

- Sécurité basée sur les grands volumes de données
- Connaissance situationnelle
- Contexte en temps réel
- Facilité de gestion
- Sécurité intégrée

Pour que les solutions SIEM puissent véritablement contribuer à l'optimisation des stratégies de gestion de la sécurité et des risques, notamment en ce que concerne la protection contre les menaces, l'adoption des nouvelles tendances et l'alignement avec les priorités métier, il est essentiel de résoudre ces cinq problèmes. Cette présentation décrit ces différents problèmes et propose une étude de cas et un scénario d'utilisation pour chacun.

1. Sécurité basée sur les grands volumes de données

La sécurité basée sur les grands volumes de données peut s'avérer extrêmement utile pour autant que vous soyez à même de l'exploiter. Les anciennes solutions SIEM n'ont pas été conçues pour intégrer un tel nombre de postes clients, de réseaux et de sources de données, pas plus qu'elles n'étaient destinées à gérer des volumes d'événements d'une telle ampleur ni des stratégies de conservation d'une durée aussi longue. Par conséquent, les bases de données relationnelles et d'autres lacunes similaires des anciennes solutions SIEM, essentiellement conçues pour gérer les événements réseau, ne répondent pas aux besoins de sécurité des infrastructures informatiques dynamiques d'aujourd'hui. Leur vitesse ainsi que leurs possibilités d'extension et d'évolutivité sont trop limitées pour qu'elles soient efficaces et présentent une véritable utilité.

Scénario d'utilisation — sécurité basée sur les grands volumes de données

- Etendez la capture des données grâce à des informations plus complètes transmises par un nombre accru de sources.
- Procédez à des analyses et à des investigations numériques de gros volumes de données.
- Optimisez votre environnement afin qu'il réponde aux exigences de la sécurité basée sur de grands volumes de données en termes de vitesse et de volume.
- Améliorez l'efficacité du personnel et des processus.

Etude de cas — secteur public

Une importante agence gouvernementale aurait voulu appliquer l'analyse avancée aux grands volumes de données de sécurité stockés dans la base de données relationnelle de plusieurs pétaoctets de sa solution SIEM. Malheureusement, il fallait des heures et parfois plus d'une journée pour générer des rapports, aussi simples fussent-ils, ce qui rendait la solution SIE inutilisable pour l'investigation numérique.

En remplaçant sa solution SIEM par McAfee® Enterprise Security Manager, l'agence a pu multiplier le nombre et les types d'équipements intégrés et enrichir ainsi ses analyses d'informations contextuelles plus complètes sur les utilisateurs et les données. Elle a pu également augmenter le volume d'événements pris en charge et de données stockées. A présent que les rapports sont générés en quelques minutes, elle bénéficie d'une approche réellement optimisée de l'investigation numérique.

Scénario d'utilisation — connaissance situationnelle

- Complétez la connaissance situationnelle par des solutions de gestion des identités supplémentaires.
- Bénéficiez d'informations complètes sur les utilisateurs, leurs actions, les équipements utilisés et la date et l'heure des activités.
- Identifiez les autres personnes impliquées, les activités liées et leur durée.
- Incluez les équipements personnels utilisés en entreprise, notamment les ordinateurs portables et les smartphones.

2. Connaissance situationnelle

Il fut un temps où une solution SIEM n'était qu'un simple outil destiné à mettre en corrélation les événements détectés au niveau des pare-feux et des systèmes de détection des intrusions et, dans certains cas, à appliquer des données d'évaluation des vulnérabilités. Aujourd'hui encore, certaines solutions SIEM continuent de s'appuyer essentiellement sur les données des flux réseau. Bien que ces différentes sources soient importantes, il est nécessaire de les compléter par des informations contextuelles sur les applications, les données et l'identité. Sans cela, il faut davantage de temps et de ressources pour recueillir suffisamment de connaissances situationnelles afin de comprendre les événements, de les hiérarchiser en fonction de leur gravité et d'y réagir.

Etude de cas — prestataire de soins de santé

Un prestataire de soins de santé régional, séduit par l'idée d'utiliser des équipements personnels sur le lieu de travail pour améliorer l'agilité du personnel, avait décidé d'autoriser l'usage des tablettes personnelles. Cela étant, en raison d'incidents passés, le prestataire s'inquiétait des risques d'utilisation abusive des informations par le personnel. Sa précédente solution SIEM n'était pas en mesure d'identifier les utilisateurs qui accédaient aux informations sensibles, et ce quel que soit l'équipement utilisé (ordinateur portable, poste de travail, tablette ou poste de travail virtuel).

Avec McAfee Enterprise Security Manager, le prestataire a pu intégrer des produits de gestion des identités et de la mobilité et des services Active Directory et LDAP pour recueillir des informations sur les utilisateurs et les équipements. Grâce à l'intégration de banques de données structurées et non structurées (prise en charge de bases de données natives, par exemple) et de solutions de prévention des fuites de données (DLP) et de surveillance de l'activité des bases de données (DAM), il a pu disposer d'une connaissance situationnelle plus complète et d'une meilleure protection contre les menaces internes.

Scénario d'utilisation — contexte en temps réel

- Identifiez les menaces internes et externes à l'environnement.
- Complétez les renseignements fournis par la solution SIEM par un contexte en temps réel.
- Limitez le temps nécessaire à l'identification des incidents et aux interventions.
- Identifiez et hiérarchisez les menaces en recourant à d'autres sources d'informations de sécurité.

3. Contexte en temps réel

Au départ, les solutions SIEM étaient surtout utilisées pour la gestion des journaux, c'est-à-dire pour collecter et stocker des données, exécuter des requêtes ou, parfois, générer quelques notifications et alertes. Si les journaux demeurent un composant essentiel d'une solution SIEM, celle-ci doit aujourd'hui également bénéficier d'un contexte en temps réel.

Ce contexte, c'est à des solutions telles que McAfee Global Threat Intelligence (McAfee GTI) et McAfee Vulnerability Manager qu'elle le doit. McAfee GTI propose un service de réputation en temps réel basé dans le cloud, et McAfee Vulnerability Manager collecte des informations organisationnelles sur les vulnérabilités des ressources.

Etude de cas — chaîne de la grande distribution

Une chaîne de magasins figurant au classement Fortune 100 qui ne possédait pas de solution SIEM de production ni de produits McAfee a réalisé une preuve du concept. Au cours de la première semaine, elle s'est rendu compte que plus de 30 % du trafic tentant d'accéder à son réseau provenaient de sources malveillantes et/ou contenaient une charge active malveillante.

En utilisant McAfee Enterprise Security Manager pour corréler les informations des événements avec McAfee GTI, la chaîne a rapidement identifié les ressources ciblées dans tous ses magasins et centres de données et a pu mieux comprendre les types d'attaques lancées à son encontre. La solution McAfee SIEM a pu déterminer les problèmes les plus graves et les mesures à appliquer en priorité. Couplée à un contexte en temps réel, elle a permis d'accélérer la détection des menaces, leur hiérarchisation et l'application de contre-mesures.

Scénario d'utilisation — facilité de gestion

- Déployez une solution SIEM avec des listes d'autorisation dynamiques et une sécurité assistée par le matériel pour protéger les équipements à fonction fixe.
- Simplifiez les investigations numériques grâce à des fonctions d'accès aux détails personnalisables.
- Intégrez la solution SIEM avec un pare-feu et un système de prévention des intrusions (IPS) pour accélérer la réponse en cas d'incident.
- Prolongez la durée de vie des ressources plus anciennes grâce à une sécurité renforcée.

4. Facilité de gestion

Les anciennes solutions SIEM possèdent des architectures très rigides et sont dépourvues de quelques fonctionnalité essentielles. Ainsi, il est difficile de les intégrer avec des équipements jusque-là non pris en charge afin de pouvoir exploiter les informations. En revanche, les solutions SIEM de nouvelle génération sont simples à personnaliser et suffisamment souples pour s'adapter à n'importe quel environnement. C'est précisément la raison pour laquelle le déploiement d'une solution SIEM de nouvelle génération revêt une importance stratégique pour tant d'organisations.

Etude de cas — société de services publics

Une importante compagnie de distribution d'électricité devait implémenter des contrôles de sécurité pour empêcher des attaques similaires à Stuxnet de mettre à mal son infrastructure et de plonger des millions de clients dans le noir. Avec McAfee Enterprise Security Manager, la compagnie a pu bénéficier d'une connaissance situationnelle des différentes zones de son environnement — réseau informatique d'entreprise, système SCADA et système de contrôle industriel (ICS) — avec prise en charge native des équipements, des applications et des protocoles.

La solution McAfee SIEM a offert au client les outils nécessaires pour entreprendre sa propre intégration personnalisée avec les systèmes SCADA et ICS. Grâce à cela, il lui a été possible d'implémenter des fonctions de corrélation, de détection des anomalies et d'analyse des tendances au niveau des trois

zones. Outre la collecte personnalisée d'événements, le client a pu rapidement et facilement créer des tableaux de bord, des rapports, des règles de corrélation et des alertes uniques. La solution est ainsi devenue un outil précieux pour gérer la sécurité, prouver la conformité aux exigences réglementaires et assurer la disponibilité des ressources — pour que la lumière continue de briller.

Scénario d'utilisation — sécurité intégrée

- Optimisez le flux des opérations et de la sécurité.
- Réduisez la complexité grâce à l'automatisation et à une personnalisation aisée.
- Améliorez la visibilité et la connaissance situationnelle à l'aide de solutions de sécurité qui fonctionnent de concert.
- Bénéficiez d'une sécurité optimisée grâce aux renseignements recueillis et à l'intégration des produits.

5. Sécurité intégrée

Certes, un produit SIEM constitue un composant important de n'importe quel projet de sécurité stratégique, mais il est loin d'être le seul. L'intégration de différentes solutions de sécurité et de conformité garantit des performances bien meilleures que les solutions individuelles, sans compter qu'une architecture non intégrée est source de complexité. Cette complexité est la raison pour laquelle la sécurité reste souvent largement tactique au lieu de devenir plus stratégique et d'être mieux alignée sur les priorités métier.

Etude de cas — services financiers

Une banque multinationale était à la tête d'un véritable arsenal de produits disparates provenant de multiples fournisseurs. Certains de ces produits étaient opérationnels, mais beaucoup n'étaient pas régulièrement utilisés ni gérés par manque de ressources. La banque a constaté qu'en utilisant la solution SIEM en combinaison avec des contrôles intégrés des données, du réseau et des postes clients, elle pouvait réduire plus efficacement les risques et les coûts, mais également bénéficier d'une sécurité plus adaptée à ses activités.

La banque a réduit le nombre de fournisseurs et réalisé d'importantes économies d'échelle. Elle a pu diminuer les coûts de formation et le nombre d'agents, de consoles, de serveurs, etc. Elle a également réduit les coûts des contrats et de multiples dépenses connexes. Outre les économies réalisées, la banque a fait en sorte que toutes les solutions en place et à venir soient totalement intégrées avec McAfee Enterprise Security Manager de façon à bénéficier de contrôles plus efficaces et d'une visibilité accrue sur sa sécurité.

Considérations essentielles

- Dans quelle mesure est-il important pour vous de pouvoir gérer facilement les défis présentés par les grands volumes de données exploités à des fins de sécurité, à savoir la collecte, le stockage, l'accès, le traitement et l'analyse ?
- Les parties prenantes à la sécurité de votre entreprise disposent-elles des informations requises au moment voulu pour prendre des décisions avisées et appliquer les mesures nécessaires ?
- Votre équipe de sécurité a-t-elle accès au contexte en temps réel dont elle a besoin pour identifier les risques et les attaques avant qu'ils ne puissent entraîner des dommages ?
- Quel serait l'impact sur la sécurité et les ressources si vous utilisiez une solution SIEM dotée de fonctions d'accès aux détails intuitives et de vues facilement personnalisables ?
- En quoi l'intégration de votre infrastructure améliorerait-elle votre sécurité, votre visibilité, vos processus et votre réactivité ?

Les fonctions offertes par les solutions SIEM d'ancienne génération ces dix dernières années ne répondent plus aux besoins actuels. Les nouvelles exigences liées aux grands volumes de données, aux informations de sécurité, à la connaissance situationnelle, aux performances, à la convivialité et à l'intégration ont conduit à une multiplication des scénarios d'utilisation des solutions SIEM. Celles-ci doivent réduire la complexité et non l'accroître. Exigez plus de votre solution SIEM.

Aujourd'hui, les solutions SIEM doivent s'intégrer à une infrastructure de sécurité plus vaste et mieux connectée au sein de laquelle la sécurité est alignée sur les priorités de l'entreprise. Elles jouent un rôle clé dans la mise en place d'une sécurité plus stratégique et l'apport d'une réelle valeur à l'entreprise.

Pour en savoir plus sur les solutions SIEM de McAfee, visitez notre site à l'adresse : www.mcafee.com/fr/products/siem/index.aspx.

Security Connected

La plate-forme Security Connected de McAfee offre une infrastructure unifiée regroupant des centaines de produits, services et partenaires afin d'exploiter leurs connaissances respectives, de partager des données contextuelles en temps réel et de collaborer pour protéger les informations et les réseaux. Toute entreprise peut améliorer son niveau de protection et réduire ses charges d'exploitation grâce aux concepts novateurs de la plate-forme, à des processus optimisés et à des économies concrètes.

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

61099brf_focus-5-siem_0514_fnl_ETMG