Guide des solutions SIEM

Qu'est-ce qu'un SIEM ?

Tout commence souvent par un incident minime qui passe inaperçu. Un lien de phishing envoyé à un nouvel employé, une attaque d'ingénierie sociale par téléphone visant une assistante de direction, une clé USB branchée sur un PC non surveillé dans un hall d'entrée, un serveur sur lequel aucun correctif n'a été installé et exécutant un vieux logiciel, ou une imprimante réseau obsolète exposée à Internet. Et avant même de vous en rendre compte, vous êtes victime d'une attaque par rançongiciel à grande échelle ou d'une violation de données causant des pertes financières importantes, affectant la confiance de vos clients et causant d'autres dommages irréparables.

Il ne fait aucun doute que la cybercriminalité a considérablement augmenté au cours des deux dernières décennies et qu'elle a gagné en complexité et en sophistication, ce qui en fait l'un des principaux risques à maîtriser pour toute entreprise.

Pour lutter contre cette complexité persistante et cette nouvelle tendance à grande échelle, les professionnels de la cybersécurité se tournent vers des logiciels de pointe qui surveillent et analysent la télémétrie et les journaux des infrastructures informatiques en temps réel, afin de détecter les irrégularités et les modèles susceptibles d'indiquer des menaces réelles. On appelle ce type de solution « système de gestion des informations et des événements de sécurité » (Security Information and Event Management, SIEM). Ce système est considéré comme un composant essentiel de tout écosystème de cybersécurité et comme un outil de conformité indispensable.

Les solutions SIEM sont apparues il y a plus de dix ans et évoluent rapidement, au rythme d'un paysage de plus en plus complexe et problématique en matière de cyber-risques.

Comment un système SIEM fonctionne-t-il ?

Un système SIEM recueille et analyse les journaux d'événements de sécurité provenant de divers points de données, notamment les serveurs, les postes de travail, les applications logicielles, le stockage, le trafic réseau, en plus des périphériques réseau et périphériques de sécurité. Le SIEM normalise ensuite ces données, dont le format et la structure varient généralement, puis les analyse en temps réel. Il met ensuite les données en corrélation afin de détecter toute activité suspecte et tout incident susceptible de représenter une menace réelle, et évalue leur gravité et leur impact potentiels.

Les systèmes SIEM permettent d'automatiser le traitement et la manipulation d'importants volumes de données provenant de sources multiples, d'une manière que l'homme est incapable de reproduire, tout en bénéficiant de sources externes d'informations sur les menaces. L'apprentissage automatique et l'intelligence artificielle ajoutent une couche supplémentaire d'efficacité aux systèmes SIEM, en leur permettant d'analyser les jeux de données volumineux afin de détecter des anomalies qui ne semblaient pas jusque-là suggérer la présence de menaces, ou d'évaluer par exemple le comportement des utilisateurs afin de détecter des menaces internes.

Le facteur humain joue toujours un rôle essentiel dans une configuration SIEM. Il intervient généralement sous la forme d'un Centre opérationnel de sécurité (Security Operations Centre, SOC), au sein duquel les équipes d'experts en cybersécurité sont alertées de menaces potentielles, enquêtent sur ces incidents selon le contexte, déterminent la bonne marche à suivre et interviennent en temps réel.

Tous les journaux capturés dans un système SIEM sont stockés pendant une période définie pour des raisons de conformité réglementaire et dans le but d'effectuer d'autres analyses si nécessaire.

Options d'acquisition et de déploiement d'un SIEM

Un SIEM est essentiellement une solution logicielle qui peut être acquise et déployée de trois façons différentes :

SIEM sur site

Dans le cadre d'une solution SIEM sur site, vous vous procurez le logiciel, le matériel et les ressources, et déployez le système au sein de votre propre infrastructure informatique. Cette approche vous permet d'avoir un contrôle total sur le déploiement et de conserver les données en interne. Cependant, cela signifie également que vous êtes entièrement responsable de la maintenance et de la gestion du système, ce qui nécessite généralement beaucoup de ressources. Un phénomène courant engendré par ce type de mise en œuvre est la fatigue associée aux alertes : vos équipes internes sont inondées d'alertes, y compris des faux positifs qui doivent être analysés de façon plus approfondie pour confirmation. De plus, cette option affiche souvent le coût total de possession (CTP) le plus élevé par rapport aux autres méthodes.

SIEM dans le cloud

Dans le cadre d'un SIEM cloud, l'abonnement est facturé à l'utilisation, ce qui évite de devoir acheter et configurer le logiciel et le matériel, et réduit ainsi les coûts initiaux. Avec cette approche, le coût dépend de plusieurs combinaisons de variables telles que le volume, les ressources, le nombre de périphériques ou la vélocité des données. Très souvent, lorsque le SIEM est basé dans le cloud, les données des journaux sont stockées et traitées hors site, ce qui peut constituer un défi pour beaucoup en matière de conformité. Un autre défi majeur du SIEM cloud est qu'il nécessite encore beaucoup de ressources et d'expertise pour surveiller le système, répondre aux alertes et faire évoluer le système afin de pouvoir gérer de nouveaux cas.

SIEM infogéré

Dans le cadre d'une approche SIEM infogérée, la solution SIEM est acquise en tant que service infogéré, fourni par une société tierce expérimentée dans la mise en œuvre et l'exploitation de systèmes SIEM et la gestion d'activités de détection des menaces et d'intervention. Une solution SIEM infogérée regroupe à la fois le système SIEM et les services professionnels sous forme d'offre personnalisée. Il est important de faire la distinction avec les services professionnels tiers acquis séparément pour faciliter la prise en charge d'un nouveau déploiement SIEM ou d'un déploiement existant, sur site ou dans le cloud, en particulier lorsqu'il s'agit de comparer les coûts.

Bien que cette approche offre moins de contrôle, elle engendre des coûts moins élevés et nécessite moins d'embauches en interne. Elle est donc plus accessible à plus grand nombre d'entreprises qui peuvent ainsi profiter des avantages d'un système SIEM sans avoir à l'acheter ou à en assurer la gestion.

Quelle est la meilleure approche à suivre ?

Le choix idéal lorsqu'il s'agit de déployer un SIEM dépend de nombreux facteurs tels que le champ de surveillance, vos propres priorités et exigences, les exigences de conformité réglementaire, la capacité et l'expérience de vos équipes de sécurité en interne, et bien sûr les restrictions budgétaires.

Dans le cas de la plupart des PME, le champ de surveillance est plus restreint, les équipes internes sont plus petites et ont des capacités réduites, et les budgets sont généralement inférieurs : un SIEM basé dans le cloud ou un SIEM infogéré s'avère alors l'approche idéale. Alors que dans le cas des grandes entreprises, la portée de la surveillance est généralement beaucoup plus large, les équipes internes sont plus nombreuses et plus performantes, et les budgets sont plus élevés : un SIEM sur site ou un SIEM complet dans le cloud est donc l'approche idéale.

Néanmoins, il peut être plus efficace pour les grandes entreprises d'utiliser une solution SIEM infogérée comme le suggèrent les données de terrain. Selon Gartner, principal cabinet de conseil et de recherche dans le domaine des technologies de l'information, de nombreuses entreprises cherchent à obtenir un support externe pour accompagner leur déploiement SIEM, ou prévoient d'acquérir ce service de support lors de l'achat d'un produit SIEM. Beaucoup d'entre elles indiquent manquer de ressources internes pour gérer un déploiement SIEM ou surveiller les alertes en temps réel, ou ne disposent pas des compétences nécessaires pour faire évoluer un déploiement dans le cadre de nouveaux cas d'utilisation.

Gartner annonce une hausse constante de la demande en matière de services SIEM infogérés. De plus en plus de clients sont en effet confrontés à des exigences de surveillance continue et mettent en œuvre des cas d'utilisation qui nécessitent une expertise SIEM opérationnelle et analytique plus poussée.

Par conséquent, dans la plupart des cas, une approche SIEM infogérée reste le choix logique pour les sociétés dont le budget est limité (peu importe le type et la taille de l'entreprise) et qui ne disposent pas d'une équipe dédiée d'experts en sécurité capables de déployer et de gérer une solution SIEM et de répondre au volume important d'alertes que la solution est susceptible de générer.