APPROCHE SIEM AVANCÉE DE RSA NETWITNESS® PLATFORM

PRÉSENTATION

Depuis l'avènement du numérique, la sécurité des informations représente un défi majeur pour les organisations. Aujourd'hui cependant, plusieurs facteurs compliquent encore la sécurité :

- La transition rapide du secteur vers une infrastructure virtualisée et basée sur le Cloud a démantelé l'approche de sécurité traditionnelle basée sur le périmètre.
- Des cybermenaces ont été commercialisées à des fins d'utilisation massive, avec de nombreux exploits provenant d'organisations de renseignement nationales.
- La gestion du cyber-risque est devenue une responsabilité métier clé, pas seulement un problème IT.

RSA reconnaît et comprend ces défis et propose des outils et services avancés de gestion SIEM et de défense contre les menaces qui aident les organisations à détecter et à répondre rapidement aux menaces dans cet environnement en constante évolution.

La gestion des événements et des informations de sécurité (SIEM) avancée accélère la détection et la réponse face aux menaces, apporte une visibilité supplémentaire et approfondie, et intègre à la fois l'intelligence sur les menaces et le contexte métier pour vous aider à hiérarchiser les menaces et les incidents de sécurité. Elle apporte les avantages suivants :

- Une visibilité inégalée pour détecter les menaces où qu'elles se trouvent
- Des fonctionnalités pour détecter instantanément toute l'étendue d'une attaque
- Un contexte métier permettant aux analystes de répondre rapidement aux menaces les plus importantes

Qu'il s'agisse du résultat de cybercriminels lançant des attaques de phishing ou de programmes malveillants qui utilisent la messagerie électronique d'une entreprise, d'états ciblant la propriété intellectuelle de sociétés ou d'utilisateurs internes faisant mauvais usage de données sensibles, nous vivons dans un monde dans lequel il est devenu quasiment impossible de prévenir les violations de données. Compte tenu de la rapidité à laquelle les cybercriminels sont en mesure de créer et d'exécuter de nouvelles menaces de sécurité dans le monde entier, les entreprises doivent changer leur approche en matière de sécurité.

POURQUOI UNE APPROCHE SIEM AVANCÉE EST-ELLE NÉCESSAIRE ?

La sophistication des acteurs malveillants et la surface d'attaque en constante expansion d'une infrastructure IT moderne ont évolué au-delà des fonctionnalités des approches SIEM existantes et des outils associés. Les équipes de sécurité ont besoin d'être capables de détecter rapidement les compromissions et de comprendre leur étendue, afin de pouvoir réagir avant que ces menaces n'affectent l'entreprise.

Les pirates sont en mesure d'accéder à l'infrastructure d'une organisation plus vite que jamais (généralement en quelques minutes) et la plupart d'entre eux extraient des données sensibles en quelques heures. Cependant, des semaines voire des mois peuvent être nécessaires pour détecter ces mêmes violations et généralement pas par des contrôles et des systèmes de sécurité internes, mais plutôt par des sources externes telles que les clients ou les autorités.

Les organisations ont du mal à détecter et à répondre rapidement en raison des éléments suivants :

- Dépendance disproportionnée vis-à-vis des contrôles préventifs
- Angles morts au niveau du réseau, des points de terminaison et de l'infrastructure virtuelle et Cloud
- Flot de données provenant de sources de données en silos, avec une analytique ou des corrélations limitées ou inexistantes entre elles
- Manque d'intelligence dynamique sur les menaces et de contexte métier pour enrichir leurs données de sécurité
- Ressources inexpérimentées et rares en termes d'analystes

Le paysage des menaces est plus sophistiqué :

- Au fur et à mesure que les entreprises migrent les applications, les données et l'informatique au quotidien vers le Cloud, elles acquièrent une infrastructure évolutive, mais sont plus vulnérables et ont une visibilité limitée sur les événements qui se produisent en dehors des environnements réseau traditionnels.
- Les attaquants sont bien renseignés, ciblés et comprennent les angles morts des organisations.
- Les attaquants n'ont besoin d'avoir raison qu'une seule fois. Les équipes de sécurité doivent avoir raison à chaque fois.

Les équipes de sécurité ont du mal à être efficaces en matière de détection et de réponse :

- Les experts techniques ont du mal à suivre le flot d'alertes qui ont une hiérarchisation limitée.
- Les analystes de la sécurité s'appuient sur des corrélations, des détections et des investigations manuelles.
- Il faut trop de temps pour comprendre comment les incidents de sécurité affectent l'ensemble de l'activité.

L'approche SiEM avancée de RSA NetWitness Platform est une solution de détection et de réponse aux menaces permettant aux équipes de sécurité d'effectuer une évaluation complète, puis d'éradiquer les menaces avant qu'elles n'aient un impact sur votre activité.

- Visibilité sur tous les systèmes pour détecter rapidement les menaces
- Alignement entre le contexte métier et les risques de sécurité, en corrigeant les lacunes des solutions purement technologiques
- Assurance de bien comprendre toute l'étendue de la menace
- Optimisation de l'efficacité en automatisant les flux de travail des analystes et en soutenant les objectifs de conformité
- Détection complète des menaces inconnues en fonction du comportement. Authentification basée sur les menaces pour définir des politiques d'authentification qui agissent sur une activité suspecte et optimisent la confiance.

197

JOURS

Temps moyen nécessaire aux organisations pour identifier une violation

Source : *Étude 2018, Ponemon Institute, Coût d'une violation de données*

APPROCHE SIEM AVANCÉE DE RSA NETWITNESS PLATFORM

L'approche SIEM avancée de RSA NetWitness Platform permet aux équipes de sécurité de détecter et de comprendre toute l'étendue d'une compromission, car elle analyse les données et le comportement des journaux, des paquets et des points de terminaison de l'entreprise, ainsi que le comportement des personnes et des processus sur le réseau. La solution transforme ces données en renseignements exploitables sur les menaces à l'aide d'un enrichissement en temps réel avec un contexte métier et une intelligence sur les menaces provenant de diverses sources. L'approche SIEM avancée crée une taxonomie unifiée de toutes ces données intelligentes afin d'accélérer la détection des menaces connues et inconnues.

L'approche SIEM avancée de RSA NetWitness Platform propose des fonctionnalités puissantes basées sur l'apprentissage machine, l'analytique du comportement des utilisateurs et des entités (UEBA), les règles de corrélation et l'intelligence avancée sur les menaces. L'approche SIEM avancée de RSA NetWitness Platform fournit une orchestration et un flux de travail basés sur les rôles pour les activités de détection et de réponse face aux menaces, ainsi que des modèles de déploiement flexibles (via le Cloud, la virtualisation, les appliances) pour prendre en charge l'infrastructure IT moderne.

Cette plate-forme complète et flexible permet à l'approche SIEM avancée de RSA NetWitness Platform d'optimiser considérablement les processus de détection et de réponse face aux menaces. Dans un environnement où l'expertise en matière de sécurité est rare et coûteuse, l'approche SIEM avancée de RSA NetWitness Platform maximise l'efficacité des analystes de la sécurité pour protéger leurs organisations contre les cybermenaces avancées.

Voici quelques-unes des fonctionnalités clés de l'approche SIEM avancée de RSA NetWitness Platform :

- **Plate-forme unifiée et unique pour toutes vos données.** Il s'agit de la seule solution qui combine l'analytique de la détection des menaces, la surveillance des journaux et des événements, ainsi que la visibilité sur les points de terminaison et le réseau avec des fonctionnalités d'investigation et d'intelligence sur les menaces pour toutes vos données. Avec l'analyse dynamique, l'approche SIEM avancée de RSA NetWitness Platform offre une valeur ajoutée instantanée aux sources nouvelles et inconnues, sans nécessiter de codage ou d'analyseurs personnalisés.
- **Contexte intégré sur les menaces et l'activité.** En ajoutant le contexte métier à l'analyse des menaces, les organisations peuvent hiérarchiser les menaces en fonction de l'impact potentiel sur leurs activités. En outre, les informations d'intelligence collectées dans le secteur de la recherche et du crowdsourcing à partir de notre base de clients et des données internes à l'organisation, sont entièrement agrégées et rendues opérationnelles au moment de l'ingestion pour une détection plus rapide des menaces.
- **Analytique intégrée du comportement.** RSA NetWitness® UEBA est une solution spécialement conçue pour l'analytique du comportement des utilisateurs et des entités, axée sur le Big Data et intégrée en tant que partie centrale de RSA NetWitness Platform. En tirant parti de la détection des anomalies statistiques non surveillées et de l'apprentissage automatique, RSA NetWitness Platform offre une détection complète et basée sur les comportements des menaces inconnues afin de répondre à un large éventail de cas d'utilisation. RSA NetWitness Platform augmente la capacité de votre équipe de sécurité existante grâce à une détection rapide et des renseignements exploitables à chaque étape du cycle de vie de l'attaque.

- **Investigations rapides.** L'approche SIEM avancée de RSA NetWitness Platform fournit un laboratoire avancé aux analystes pour trier les alertes et les incidents, notamment une interface spécialement conçue pour les investigations de sécurité. En tirant parti des informations détaillées sur les données issues de l'ensemble de l'infrastructure, les analystes peuvent reconstruire de manière native et visuelle une attaque réseau ou une exfiltration de données dans son intégralité. L'approche SIEM avancée permet aux analystes de connecter des incidents de manière chronologique pour dévoiler et mieux comprendre l'ampleur d'une attaque.
- **Automatisation et orchestration.** RSA NetWitness® Orchestrator est une technologie d'automatisation et d'opérations de sécurité complète qui associe une gestion complète des dossiers, une automatisation et une orchestration intelligentes, ainsi que des fonctionnalités d'investigation collaborative. RSA NetWitness Orchestrator permet aux analystes du SOC de bénéficier de fonctionnalités cohérentes, transparentes et documentées en matière d'investigation et de recherche des menaces. Il permet de tirer profit des actions de réponse automatisées et basées sur un playbook, de renseignements tirés de la détection automatique et de l'apprentissage machine pour une résolution plus rapide et une meilleure efficacité du SOC.
- **Architecture flexible et évolutive.** En proposant une large gamme d'options de déploiement flexibles, l'approche SIEM avancée de RSA NetWitness Platform peut évoluer de façon incrémentielle en fonction des besoins de l'organisation et des priorités en matière de sécurité. Qu'elle soit déployée sous la forme d'une seule ou de dizaines d'appliances, de déploiements partiellement ou entièrement virtualisés, sur site ou dans le Cloud, l'approche SIEM avancée de RSA NetWitness Platform peut prendre en charge les architectures spécifiques des clients.
- **Opérations de sécurité de bout en bout.** L'approche SIEM avancée de RSA NetWitness Platform est la seule plate-forme qui unifie l'analytique, la surveillance des journaux et des événements, ainsi que la visibilité sur les points de terminaison et le réseau avec l'intelligence avancée sur les menaces et la gestion automatisée des incidents afin d'optimiser les opérations de sécurité.

LES RISQUES NUMÉRIQUES SONT L'AFFAIRE DE TOUS
VOUS AIDER À LES GÉRER, C'EST NOTRE AFFAIRE

Les solutions RSA offrent aux organisations une approche unifiée de la gestion du risque numérique qui repose sur une visibilité intégrée, des informations automatisées et des actions coordonnées. Les solutions RSA sont conçues pour détecter et traiter efficacement les attaques avancées, gérer les contrôles d'accès des utilisateurs, et réduire les risques métiers, la fraude et la cybercriminalité. RSA protège des millions d'utilisateurs dans le monde entier et aide plus de 90 % des sociétés du classement Fortune 500 à prospérer et à s'adapter en permanence au changement transformationnel.

Découvrez comment prospérer dans un monde numérique et dynamique où les risques sont élevés sur rsa.com/fr-fr