kaspersky BRING ON THE FUTURE

Comparaison entre XDR, SIEM et SOAR

Trop d'acronymes qui vous font tourner la tête ? Découvrons un peu ce qui se cache derrière ses petites lettres...

Introduction

SIEM, SOAR, MDR, EDR, EPP, XDR... êtes-vous déboussolé, perdu dans une jungle d'acronymes relatifs à la cybersécurité ? Cela est compréhensible, et c'est la raison pour laquelle nous avons élaboré et fourni ce guide utile pour découvrir quelles sont les différences entre trois les éléments les plus importants : SIEM, SOAR et XDR. D'où viennent ces acronymes ? Comment se fait-il que l'industrie ait développé ces termes déroutants et qui recoupent des notions voisines ? Ont-ils même une signification distincte ou ne sont-ils que du marketing ? Quelles sont les similitudes et les différences ? Peuvent-ils se compléter l'un l'autre, ou sont-ils tous en concurrence ?

Venez nous rejoindre dans cette quête ! Permettez-nous de prendre nos machettes de connaissances, de nous frayer un passage dans la forêt des acronymes et du jargon, pour arriver dans une clairière ouverte de vision claire !

SIEM

La gestion des événements et des informations de sécurité (SIEM) est un ensemble d'outils et de services qui combinent la gestion des événements de sécurité (SEM) et la gestion des informations de sécurité (SIM) dans une plate-forme unique. SIEM collecte, agrège, analyse et stocke les données de journaux de l'ensemble de l'infrastructure informatique en vue de divers cas d'utilisation, notamment la gestion et la conformité, ainsi que la correspondance des corrélations basée pour les activités suspectes.

Comment ça marche ?

Les premiers services SIEM ont été développés en 2005, avec l'objectif initial d'agréger et de stocker les journaux et les événements dans l'ensemble de l'infrastructure informatique d'une organisation, en incluant les terminaux, les applications et les périphériques réseau, afin d'établir des rapports de conformité. SIEM établit des corrélations sur cet ensemble de données, en recherchant des motifs ou des événements susceptibles d'indiquer un comportement suspect, et génère une alerte pour le centre d'opérations de sécurité (SOC). Les analystes de la sécurité ont rapidement entrevu la possibilité d'utiliser ces alertes non seulement à des fins de conformité et de gestion, mais également d'identifier de manière plus proactive et d'interrompre la progression d'une activité malveillante dans l'écosystème.

Limites de SIEM

Le problème était que les services SIEM n'étaient pas conçus dans un but spécifique de détection et de réponse aux incidents. De ce fait, son emploi a été un peu difficile, pour diverses raisons :

- Trop grand nombre d'alertes : l'énorme ensemble de données délivré par SIEM devait être filtré, traité et analysé manuellement, ce qui n'est pas pratique pour des analystes de la sécurité qui essayent de prévenir des attaques dans un paysage des menaces en rapide évolution.
- Aucun contexte : pour traiter des attaques nouvelles, complexes et sophistiquées, les analystes en sécurité ont besoin d'une image contextualisée et cohérente du paysage des menaces de l'organisation, plutôt que des flux de données déconnectés fournis par SIEM.
- Trop passif : blocage de processus suspects, mise en quarantaine de fichiers et autres capacités de réponse ne relèvent pas de son domaine, car ce n'est essentiellement qu'un outil d'analyse passif.

Les professionnels de sécurité ont tenté de résoudre ces problèmes en superposant des outils supplémentaires sur SIEM, ou en développant de nouvelles générations comportant des plug-ins de Machine Learning ou d'analyse comportementale. Cependant, la demande en faveur d'un outil capable de fournir de meilleures alertes de qualité et des services plus rapides avec des processus automatisés n'était pas vraiment satisfaite.

SOAR

Les outils SOAR (Security Orchestration & Automated Response) ont vu le jour en 2015 pour résoudre certains des défauts mentionnés précédemment des systèmes SIEM. Les plates-formes SOAR ingèrent des données provenant de diverses sources de l'infrastructure, notamment des systèmes de gestion et des plates-formes de Threat Intelligence, et fournissent une analyse de la priorité. Les équipes de sécurités peuvent alors configurer des réponses automatisées multi-niveaux qui font intervenir plusieurs solutions par rapport aux menaces entrantes, en utilisant l'intégration de la plate-forme SOAR d'un écosystème d'outils de sécurité connecté à des API.

Comment ça marche ?

Cette fois-ci, le nom est vraiment bien utile ! Voici pourquoi :
Les outils SOAR automatisent. Bien qu'ils soient plus connus pour leur capacité à automatiser les processus de réponse aux incidents, ces outils peuvent en fait automatiser toute une gamme de flux de travail, notamment l'analyse des vulnérabilités, l'analyse des journaux, la gestion des accès utilisateurs, le tri des menaces, etc.

Ils effectuent cela grâce à des « guides » : ensembles de règles préconfigurées déclenchées par des événements spécifiques, qui indiquent au système les étapes à entreprendre par la suite dans un flux de travail spécifique. La plupart des solutions SOAR sont livrées avec des centaines de guides prêts à l'emploi, qui couvrent les tâches les plus courantes auxquelles sont confrontées les équipes SOC. Les équipes peuvent alors configurer leurs propres guides, afin d'automatiser d'autres processus répétitifs plus particuliers qui leur sont spécifiques.

Ensuite, ils orchestrent. Alors que l'automatisation fait référence à l'exécution pilotée par une machine de tâches individuelles dans un flux de travail unique, l'orchestration correspond à la coordination de plusieurs outils et processus hétérogènes dans un flux de travail plus vaste, rassemblant toutes les données pertinentes en une plate-forme unique pour fournir des informations consolidées et exploitables.

Relation entre SIEM et SOAR

Généralement, un SIEM est utilisé de concert avec les outils SOAR pour créer en quelque sorte une relation assistant-responsable : le SIEM collecte tous les journaux, établit des corrélations entre eux pour rechercher des alertes, puis délivre ces informations dans le SOAR, qui peut alors prendre la main sur les actions de réponse.

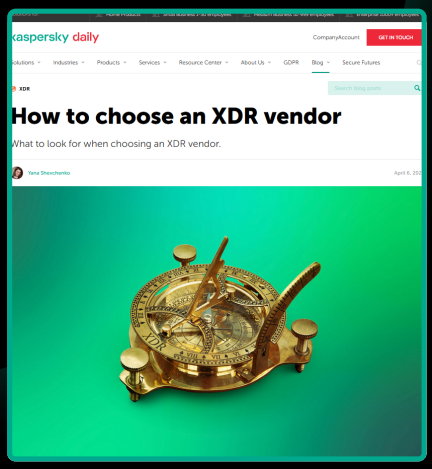
Limite du SOAR

Tout cela semble parfait, n'est-ce pas ? En fait, il apparaît que pour assurer la maintenance d'une plate-forme SOAR bien configurée qui s'intègre avec des outils de partenaires, il est nécessaire de produire un effort continu nécessitant un SOC hautement qualifié et mature, ressource dont ne disposent pas de nombreuses organisations à l'heure actuelle, étant donné le déficit de compétences en matière de cybersécurité que nous connaissons aujourd'hui.

Sans ces personnels de maintenance qualifiés et vigilants, les analystes SOAR peuvent se retrouver avec un trop grand nombre d'alertes de faible priorité, de faux positifs, et d'un ensemble de données généralement incohérentes provenant des divers des outils indépendants qui alimentent la plate-forme, ce qui est exactement ce qu'ils cherchent à éviter.

Comment choisir un fournisseur XDR ?

Plusieurs fournisseurs de cybersécurité ont pris en marche le train du XDR avec leurs propres solutions. Comment pouvez-vous savoir si vous achetez le produit adéquat ? Pour en savoir plus, découvrez notre guide : https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



XDR

XDR est une solution de sécurité sur site ou dans le cloud, généralement disponible en deux catégories : native et hybride. XDR natif est une suite unifiée d'outils d'un fournisseur unique, alors que XDR hybride intègre des solutions d'autres tiers dans votre écosystème. Le terme « XDR » a été utilisé pour la première fois en 2018, « X » signifiant « eXtended » : XDR « s'étend » au-delà des outils de détection, de réponse et de protection des terminaux traditionnels (EDR et EPP) en collectant et en effectuant des corrélations entre des données provenant de plusieurs couches, notamment la messagerie, le cloud et le réseau, afin de fournir une protection complète sur la totalité de l'infrastructure informatique.

Ainsi, il s'agit d'une plate-forme unique qui coordonne toute une gamme d'outils et qui utilise le Machine Learning et l'automatisation pour aider les équipes de sécurités à protéger la totalité de l'écosystème de sécurité… cela ressemble un peu à SOAR, non ? En fait, il existe quelques différences fondamentales. Étudions tout cela de plus près…

Comparaison entre XDR et SOAR : quelle est la différence ?

1. Les solutions XDR sont spécialisées dans les données et l'optimisation des terminaux, ce qui signifie que la détection et la réponse aux incidents est une fonctionnalité de conception centrale, qui leur procure des capacités d'analyse avancée dont ne disposent généralement pas les outils SOAR. Les outils XDR sont parfaits pour la mesure de menaces inconnues et de type zero-day, car ils tirent parti d'une intelligence artificielle puissante, d'algorithmes de Machine Learning et de la Threat Intelligence pour protéger une organisation au-delà de ses frontières. D'un autre côté, les outils SOAR peuvent offrir un éventail de cas d'utilisation beaucoup plus important, car ils orchestrent et automatisent tous les processus sur l'ensemble de l'infrastructure, et pas seulement la réponse aux incidents.
2. XDR peut être considéré comme une version allégée de SOAR : une interface simplifiée qui offre des réponses automatisées en un seul clic par rapport aux menaces et aux alertes entrantes. Cela peut être plus pratique pour une organisation qui ne dispose pas des ressources pour assurer la maintenance de la complexité d'une plate-forme SOAR bien configurée.
3. XDR permet une intégration fluide entre les produits : pour une pile d'un fournisseur unique, ou également pour des produits tiers, XDR assure parfaitement une interopérabilité transparente. Les outils SOAR ont souvent des difficultés pour essayer d'intégrer tous les outils hétérogènes et indépendants entre eux. XDR supprime ces cloisonnements pour apporter une réponse tout-en-un aux menaces.

Alors, cela signifie que XDR va remplacer SIEM et SOAR ?

La question n'est pas encore tranchée, car XDR est une technologie relativement nouvelle, qui se développe en permanence. Actuellement, la plupart des experts recommandent une approche intégrée, dans la mesure où chaque solution offre des avantages complémentaires aux autres solutions :

- SIEM : SIEM présente des cas d'utilisation en dehors de la détection des menaces, comme la gestion des journaux, la conformité et l'analyse des données non liées aux menaces.
- SOAR : la possibilité de personnalisation importante des guides SOAR est utile pour les processus d'orchestration et d'automatisation sur l'ensemble de l'infrastructure des organisations.
- XDR : lorsqu'il s'agit de détection et de réponse aux menaces, les analyses avancées d'une solution XDR offrent une protection améliorée irréprochable.

Vous recherchez une solution éprouvée, testée et adaptable pour vos experts ? Kaspersky Expert Security, XDR basé sur une solution EDR native dans le cloud, fournit à votre organisation une visibilité et des fonctionnalités améliorées pour la détection et la logique de réponses automatiques basées sur l'intelligence artificielle, sur l'ensemble des terminaux et du réseau, ce qui facilite une large gamme de scénarios automatisés de réponse aux incidents. La technologie avancée intégrée de la plate-forme pour réaliser la détection et l'analyse est assortie d'une Threat Intelligence de niveau mondial. L'architecture unifiée de la solution XDR de Kaspersky fournit une gestion centralisée à partir d'une console Web unique. Pour en savoir plus, rendez-vous sur go.kaspersky.com/expert

www.kaspersky.fr

© 2022 AO Kaspersky Lab.
Les marques déposées et les marques de service sont la propriété de leurs détenteurs respectifs.