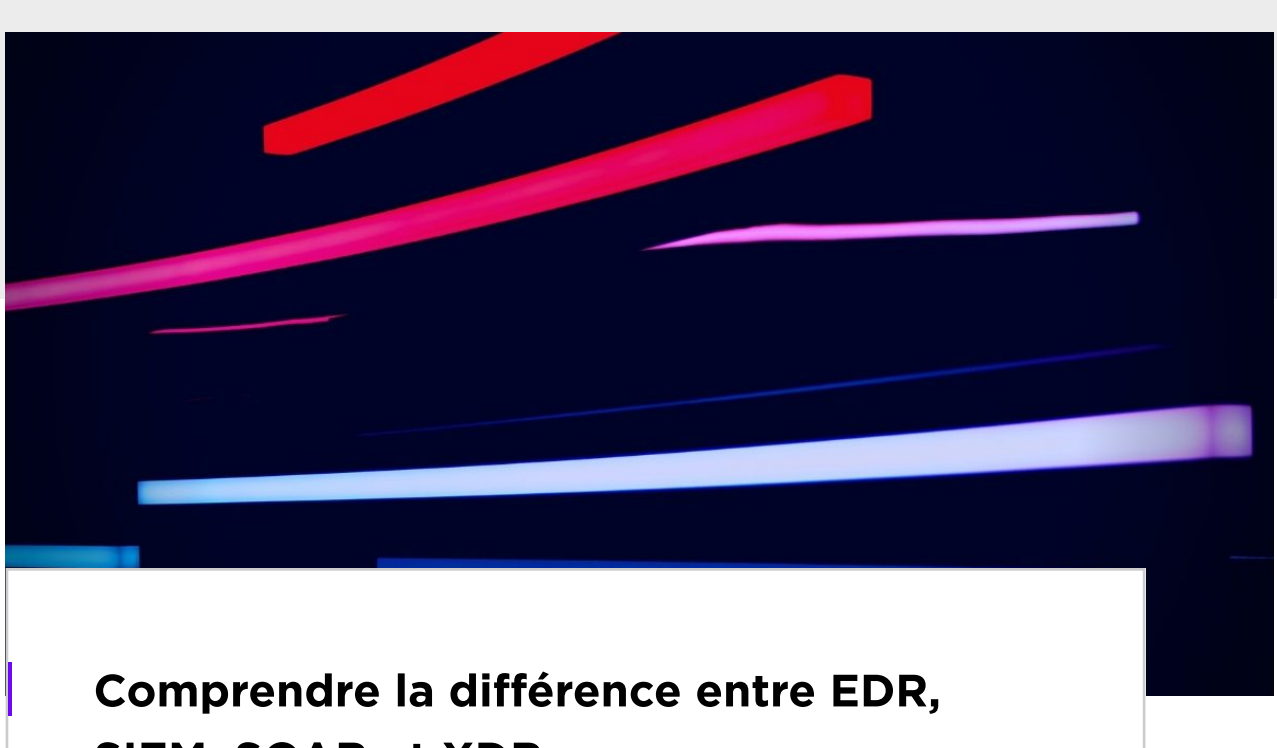


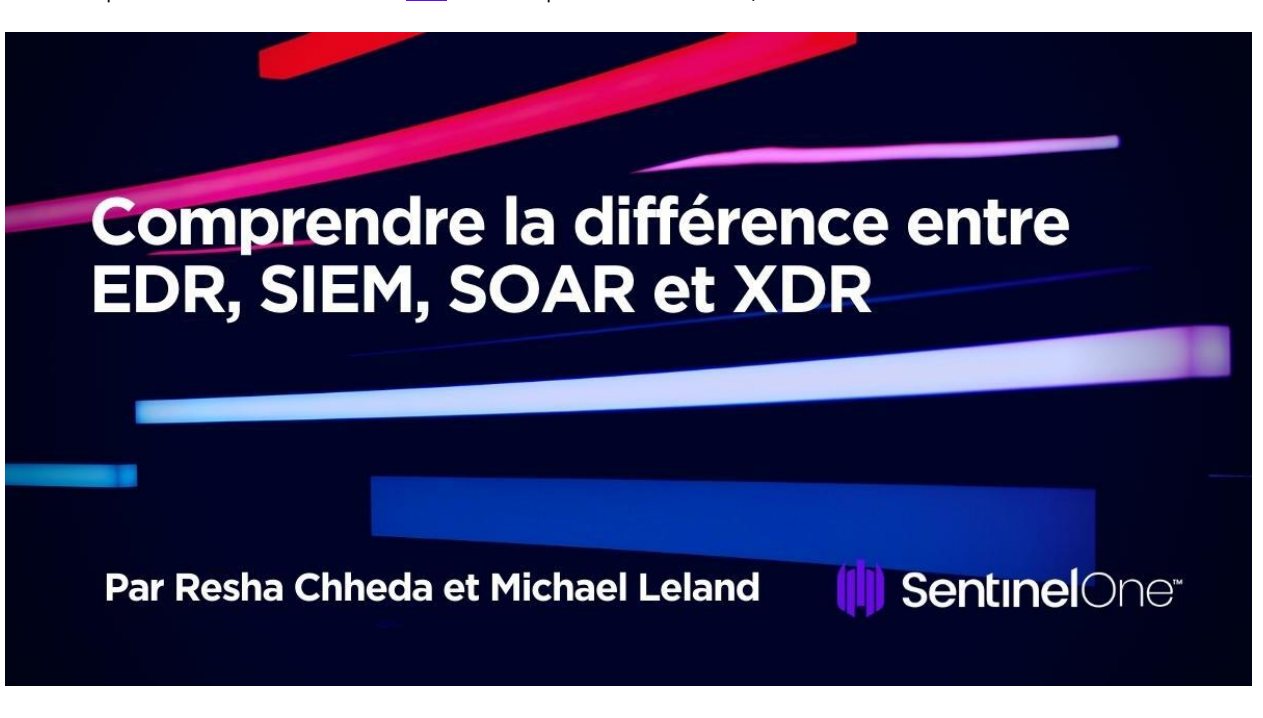
Comprendre la différence entre EDR, SIEM, SOAR et XDR

mai 11, 2022
by Resha Chheda and Michael Leland

Le monde de la cybersécurité est rempli de jargon, d'abréviations et d'acronymes. À l'heure où les vecteurs d'attaque sophistiqués se multiplient, des terminaux aux réseaux en passant par le cloud, beaucoup d'entreprises se tournent vers une nouvelle approche pour bloquer les menaces avancées. Baptisée Extended Detection and Response, cette innovation donne lieu par la même occasion à un acronyme de plus : XDR. Bien qu'il ait suscité beaucoup d'intérêt cette année auprès des leaders du secteur et de la communauté d'analystes, l'XDR reste un concept en pleine évolution. Il existe de fait une certaine confusion autour du sujet.

- Qu'est-ce que l'XDR ?
- En quoi diffère-t-il d'un EDR ?
- Est-ce l'équivalent d'un SIEM ? D'un SOAR ?

En tant que leader du marché de l'EDR et pionnier de la technologie émergente XDR, on nous demande souvent de clarifier ces concepts et la manière dont ils peuvent améliorer les résultats des clients. Cet article a pour objectif d'apporter des réponses à certaines questions courantes autour de l'XDR et sur ce qui le diffère d'un EDR, d'un SIEM et d'un SOAR.



Qu'est-ce que l'EDR ?

Un système EDR permet à une organisation de surveiller les terminaux afin de détecter tout comportement suspect, et d'enregistrer chaque activité et événement. Il corrèle les informations collectées afin de fournir un contexte critique pour la détection des menaces avancées, puis lance une réponse automatisée (par exemple, isolement d'un terminal infecté du réseau) en quasi-temps réel.

Qu'est-ce que l'XDR ?

L'XDR est une évolution de l'EDR (Endpoint Detection and Response). Tandis qu'un système EDR collecte et corrèle les activités sur de multiples terminaux, une solution XDR élargit la portée de la détection au-delà des terminaux pour fournir des capacités de détection, d'analyses et de réponse également sur les réseaux, les serveurs, les workloads cloud, les SIEM et bien plus encore.

Cette approche permet de bénéficier d'une vue unifiée et centralisée sur plusieurs outils et vecteurs d'attaque. Une visibilité ainsi améliorée permet de contextualiser ces menaces pour faciliter les tris, les investigations et accélérer les processus de remédiation.

Une solution XDR collecte et corrèle automatiquement les données sur plusieurs vecteurs de sécurité pour une détection plus rapide des menaces. Les analystes sécurité peuvent ainsi réagir rapidement avant qu'une menace ne se propage. Les intégrations prêtes à l'emploi et les mécanismes de détection prédéfinis sur divers produits et plateformes contribuent à améliorer la productivité, la détection des menaces et les investigations.

> En résumé, la technologie XDR *s'étend* au-delà des terminaux pour des prises de décision basées sur des données issues d'un plus grand nombre de produits, et peut enclencher des actions sur l'ensemble de votre pile en agissant sur la messagerie, le réseau, les identités et bien plus.

XDR et SIEM : quelle différence ?

Lorsqu'on parle d'XDR, certaines personnes pensent que c'est une autre manière de décrire un outil de gestion des informations et des événements de sécurité (Security Information & Event Management, SIEM). Or, les termes XDR et SIEM désignent deux concepts bien distincts.

Un SIEM collecte, agrège, analyse et stocke de vastes volumes de données de journaux provenant de toute l'entreprise. Il repose sur une approche initiale très large qui consiste à collecter les données de journaux et d'événements disponibles provenant de presque toutes les sources de l'entreprise afin de les stocker pour divers cas d'usage : gouvernance et conformité, correspondance de modèles basée sur des règles, détection des menaces heuristiques/comportementales (UEBA, par exemple), traque à travers les sources de télémétrie pour les indicateurs atomiques ou de compromission (IoC), etc.

Toutefois, la mise en œuvre d'outils SIEM nécessite beaucoup d'ajustements et d'efforts. Les équipes de sécurité peuvent également être submergées par l'avalanche d'alertes provenant d'un SIEM, ce qui peut conduire le SOC à ignorer les alertes critiques. En outre, même si un SIEM collecte les données de dizaines de sources et de capteurs, il reste un outil d'analytique passif qui ne fait qu'émettre des alertes.

Une plateforme XDR vise à résoudre les problématiques liées aux outils SIEM pour une détection et une réponse efficaces face aux attaques ciblées. Analytique, Threat Intelligence, profilage et analyse des comportements… elle intègre plusieurs fonctionnalités.

XDR et SOAR : quelle différence ?

Les plateformes d'orchestration, automatisation et réponse aux incidents de sécurité (Security Orchestration & Automated Response, SOAR) permettent aux équipes matures de créer et d'exécuter des playbooks multi-étapes qui automatisent les actions au sein d'un écosystème de solutions de sécurité connecté via des API. De son côté, une plateforme XDR permet d'effectuer des intégrations à l'écosystème via la Marketplace et fournit des mécanismes destinés à automatiser des actions simples par rapport à des contrôles de sécurité tiers.

Une plateforme SOAR est complexe, coûteuse et nécessite un SOC très mature pour mettre en œuvre et maintenir les intégrations et les playbooks de partenaires. L'XDR est censé être un « SOAR léger » : une solution simple, intuitive et sans code qui permet d'agir de la plateforme XDR aux outils de sécurité connectés.

Qu'est-ce que le MXDR ?

Un service managé de détection et de réponse étendues (Managed Extended Detection and Response, MXDR) étend des services MDR à l'ensemble de l'entreprise pour fournir une solution entièrement managée aux fonctionnalités multiples : analyses et opérations de sécurité, traque des menaces avancées, détection et réponse rapides sur les terminaux, le réseau et les environnements cloud, etc.

Un service MXDR augmente les capacités XDR du client par le biais de services MDR afin d'apporter des fonctionnalités supplémentaires de surveillance, d'investigation, de réponse et de traque des menaces.

XDR : pourquoi un tel buzz et un tel engouement ?

La technologie XDR remplace les environnements de sécurité cloisonnés et aide les organisations à relever les problématiques de cybersécurité autour d'une approche unifiée. Avec un pool unique de données brutes comprenant des informations provenant de tout l'écosystème, une plateforme XDR collecte des données à partir d'un plus large éventail de sources pour une détection et une réponse aux menaces plus rapides, plus approfondies et plus efficaces qu'un EDR.

L'XDR offre plus de visibilité et de contexte sur les menaces. Les incidents qui auparavant n'auraient pas été traités font l'objet d'un niveau de sensibilisation plus élevé, ce qui permet aux équipes de sécurité de remédier et réduire tout impact supplémentaire et de limiter la portée d'une attaque.

Une attaque par ransomware typique traverse le réseau, atterrit dans une boîte mail, puis infecte le terminal. Les organisations qui abordent la sécurité en examinant chacun de ces éléments indépendamment se retrouvent dans une position désavantageuse. Une solution XDR intègre des contrôles de sécurité disparates pour fournir des réponses automatisées ou en un clic sur l'ensemble du domaine de sécurité de l'entreprise (désactivation d'accès utilisateurs, forçage de l'authentification multifacteur en cas de compromission de compte suspectée, blocage des domaines entrants et des hachages de fichiers, etc.), le tout via des règles personnalisées écrites par l'utilisateur ou par la logique intégrée au moteur de réponse prescriptive.

Avec un pool unique de données brutes comprenant des informations provenant de tout l'écosystème, une plateforme XDR collecte des données à partir d'un plus large éventail de sources pour une détection et une réponse aux menaces plus rapides, plus approfondies et plus efficaces qu'un EDR.

Cette visibilité complète comporte plusieurs avantages :

- Réduction du temps moyen de détection (Mean Time To Detect, MTTD) par la corrélation des sources de données
- Réduction du temps moyen d'investigation (Mean Time To Investigate, MTTI) par une accélération des tris, des investigations et un élargissement de la portée
- Réduction du temps moyen de réponse (Mean Time To Respond, MTTR) favorisée par une automatisation simple, rapide et pertinente
- Amélioration de la visibilité sur tout le parc de sécurité

De plus, grâce à l'intelligence artificielle (IA) et à l'automatisation, l'XDR permet de réduire la charge de travail manuel des analystes sécurité. Une solution XDR détecte les menaces sophistiquées de façon rapide et proactive, ce qui améliore la productivité de l'équipe SOC ou de sécurité et augmente considérablement le retour sur investissement de l'organisation.

Conclusion

Naviguer dans le paysage des fournisseurs est un défi pour de nombreuses entreprises, en particulier lorsqu'il s'agit de solutions de détection et de réponse. Souvent, le plus grand obstacle est de comprendre ce que chaque solution fournit, surtout lorsque les terminologies varient d'un fournisseur à l'autre et peuvent signifier différentes choses.

Toute nouvelle technologie qui émerge sur le marché génère beaucoup de battage médiatique. C'est pourquoi les acheteurs doivent se montrer prudents. La réalité est que toutes les solutions XDR ne se valent pas. SentinelOne Singularity XDR unifie et étend les capacités de détection et de réponse sur plusieurs couches de sécurité, offrant aux équipes de sécurité une visibilité centralisée et de bout en bout sur l'entreprise, des analyses puissantes et une réponse automatisée sur l'ensemble de la pile technologique.

Pour en savoir plus sur la SentinelOne Singularity Platform, contactez-nous ou demandez une démo gratuite.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Cloud : quelles sont les menaces les plus dangereuses et comment s'en protéger ?
- Six idées reçues dont doivent se méfier les conseils d'administration des entreprises
- Comment défendre l'entreprise contre les risques liés à la chaîne logistique en 2022 ?