Extended Detection and Response (XDR) – Guide pour débutants

SOPHOS
Cybersecurity evolved.

Qu'est-ce que le XDR ?

Commençons par examiner la définition de XDR, car la formulation exacte peut varier selon les personnes.

- « **Extended Detection and Response** » (détection et réponse étendues) est la définition la plus couramment utilisée, adoptée par de nombreux cabinets d'analyse et d'éditeurs de cybersécurité. Le terme « Extended » fait référence au fait d'aller au-delà des systèmes endpoint et du serveur, en intégrant des sources de données supplémentaires telles que le pare-feu, la messagerie, le Cloud, les mobiles et autres.
- « **Cross-product Detection and Response** » (détection et réponse multi-produits) est une autre formulation, qui fait référence à la combinaison de données provenant de plusieurs produits et couches de sécurité.
- La troisième interprétation utilise le « X » de XDR comme une variable mathématique qui représente toutes les sources de données exploitées au sein de la solution.

Quelle que soit la définition que vous utilisez pour XDR, elles font toutes référence et utilisent toutes les mêmes composants de base. La capacité d'accéder et d'interroger une série de sources de données pour donner à votre organisation une plus grande visibilité et un meilleur contexte.

En quoi consiste la technologie XDR ?

Le XDR est conçu pour donner aux organisations une vue d'ensemble de leur posture de cybersécurité et de leur environnement informatique, avec la possibilité de procéder rapidement à des investigations approfondies lorsque des analyses plus poussées sont nécessaires.

Selon Gartner :

« Les principales propositions de valeur d'un produit XDR sont d'améliorer la productivité des opérations de sécurité et d'améliorer les capacités de détection et de réponse en intégrant davantage de composants de sécurité dans un ensemble unifié qui offre plusieurs flux de télémétrie, en présentant des options concernant plusieurs formes de détection et en permettant de déployer simultanément plusieurs méthodes de réponse. »

Gartner, « Innovation Insight for Extended Detection and Response » (2020)

Une question fréquente est « en quoi le XDR diffère-t-il de l'EDR ? ». En effet, les solutions XDR incluent les capacités de formulation de requêtes de l'EDR (Endpoint Detection and Response). C'est-à-dire, qu'elles obtiennent des données en temps réel directement à partir d'un poste ou d'un serveur, et ont accès aux données dans le Cloud si l'appareil n'est pas connecté au réseau.

Le XDR s'appuie sur cette base solide en ajoutant davantage de données et de contexte pour augmenter la visibilité et permettre des investigations plus approfondies. La détection et la réponse aux incidents sont ainsi beaucoup plus rapides et plus précises. Les sources de données supplémentaires peuvent inclure le pare-feu, la messagerie, le Cloud et les mobiles. Par exemple, en ajoutant les données du pare-feu, il est facile de corréler la détection d'un trafic malveillant par le pare-feu avec un poste compromis, ou de voir quelle application est à l'origine de la lenteur de la connexion réseau du bureau.

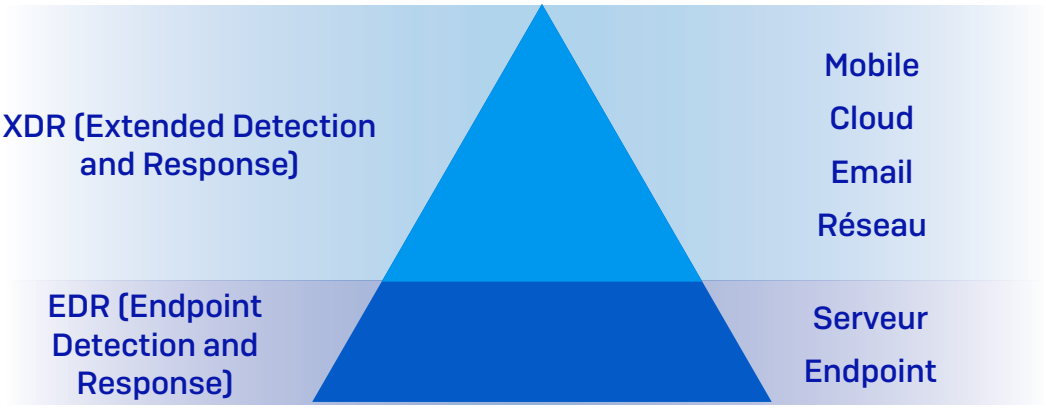
L'une des meilleures façons d'utiliser le XDR est de commencer par une « macro-analyse » qui vous donne les outils nécessaires pour analyser rapidement l'ensemble de votre environnement à la recherche d'activités suspectes, de comportements anormaux ou de tout autre problème informatique. Lorsqu'un problème est identifié, vous pouvez alors vous concentrer sur l'appareil en question, en extrayant des données en direct ou en accédant à distance à l'appareil afin de l'analyser plus en profondeur et de prendre des mesures correctives.

Sources de données étendues

Aussi puissants que soient les outils EDR, ils sont limités à la détection et la réponse aux menaces sur les postes et les serveurs. Ce n'est pas un inconvénient en soi. Si vous deviez choisir un seul endroit où concentrer vos efforts de détection et de réponse, les postes et les serveurs de votre organisation seraient un excellent choix.

Cependant, il y a des actions que vous ne pouvez pas prendre en travaillant uniquement sur ces systèmes. Après tout, votre environnement informatique est un réseau interconnecté de réseaux, d'outils de communication, d'appareils mobiles, d'applications Cloud et bien plus encore. Pour protéger votre infrastructure informatique de manière plus complète, un système intégré de détection et de réponse est essentiel. C'est là que le XDR intervient.

Le XDR est une évolution de l'EDR. Il va au-delà de la protection Endpoint et Serveur, en incorporant des données provenant d'autres outils de sécurité tels que les pare-feux, les passerelles de messagerie, les outils de Cloud public et les solutions de gestion des menaces mobiles. Le XDR étant une technologie émergente, les sources de données et les fonctionnalités varient selon les éditeurs, mais le schéma cièdessous est un bon point de départ pour comprendre comment le XDR renforce l'EDR.



Cas d'usages du XDR

La meilleure façon d'expliquer les avantages concrets du XDR est d'examiner comment cette fonctionnalité peut aider les organisations dans leurs opérations informatiques quotidiennes et leurs capacités de traque des menaces. Notez que nous avons inclus des exemples d'EDR car votre solution XDR devrait également couvrir ces cas d'usages.

	Opérations informatiques	Traque des menaces
EDR	• Pourquoi une machine est-elle lente ? • Quel appareil a des vulnérabilités connues, des services inconnus ou des extensions de navigateur non autorisées ? • Des programmes en cours d'exécution devraient-ils être supprimés ?	• Quels sont processus qui tentent d'établir une connexion réseau sur des ports non standards ? • Afficher les processus qui ont récemment modifié des fichiers ou des clés de registre • Lister les indices de compromission (IoC) mappés au cadre MITRE ATT&CK
XDR	• Identifier les appareils non gérés, invités et IoT • Pourquoi la connexion au réseau du bureau est-elle lente ? Quelle application en est la cause ? • Revenir 30 jours en arrière pour détecter toute activité inhabituelle sur un appareil disparu ou détruit	• Prolonger l'investigation jusqu'à 30 jours sans remettre un appareil en ligne • Utiliser les détections ATP et IPS du pare-feu pour analyser les hôtes suspects • Comparer les informations de l'en-tête de l'email, les algorithmes de hachage SHA et autres IoC pour identifier le trafic vers un domaine malveillant

Comment Sophos peut vous aider

Sophos XDR offre aux organisations une vue large et complète de l'ensemble de leur environnement de cybersécurité, avec la possibilité de l'analyser en profondeur si nécessaire. En d'autres termes, vous disposez à la fois d'une vue macroscopique et d'une vue microscopique sur votre environnement selon vos besoins.

Les solutions compatibles XDR envoient les données des systèmes endpoint, des serveurs, des pare-feux, de la messagerie et d'autres sources de données* au Data Lake de Sophos, un référentiel de données dans le Cloud qui contient les données critiques XDR et les données des appareils hors ligne. Il s'agit d'un lieu centralisé d'investigation pour toutes les données XDR afin que vous puissiez répondre rapidement aux questions critiques de l'entreprise, corréler les événements provenant de différentes sources de données et prendre des mesures plus éclairées.

La prise en main est simple, avec une bibliothèque de requêtes pré-écrites et entièrement personnalisables. Vous pouvez ainsi choisir une catégorie, ajouter des appareils et commencer à répondre aux questions relatives aux opérations informatiques et à la traque des menaces.

Gartner Innovation Insight for Extended Detection and Response, Peter Firstbrook, Craig Lawson, 19 mars 2020.

Gartner ne fait la promotion d'aucun fournisseur, produit ou service cité dans ses publications de recherche, et ne conseille aucunement aux utilisateurs de technologies de ne sélectionner que les fournisseurs ayant obtenu les meilleures notes ou toute autre distinction. Les publications de recherche de Gartner reflètent les opinions de l'organisme de recherche Gartner et ne devraient pas être interprétées comme un énoncé de faits. Gartner exclut toute garantie explicite ou implicite concernant cette recherche, y compris toute garantie de qualité marchande et d'adéquation à un usage particulier.

*Bientôt disponible avec Cloud Optix et Sophos Mobile

Pour en savoir plus, rdv sur Sophos.fr/xdr

SOPHOS

21-04-06 WP (NP)