

EN QUOI CONSISTE

EXACTEMENT LE XDR ?

Le XDR (eXtended Detection and Reponse) est la solution de nouvelle génération pour lutter contre les menaces sophistiquées actuelles.

Son approche globale optimise l'assimilation des données de sécurité, les analyses et les flux de travail à l'échelle du dispositif de sécurité complet d'une entreprise.



eXtended

Boostez votre EDR (Endpoint Detection and Response) grâce à une télémétrie complète, pleinement intégrée et extrayant les données de tous les composants de votre dispositif de sécurité.



Detection

Identifiez et traquez les menaces plus rapidement grâce à des indicateurs d'attaque, des informations pertinentes et des alertes inter-plateformes accessibles via une console unifiée.



Response

Utilisez les informations fournies par le XDR pour déclencher des actions orchestrées. Concevez et automatisez des flux de travail d'intervention multi-plateforme pour une correction chirurgicale et optimisée.

POURQUOI ADOPTER LE XDR SANS ATTENDRE ?

Les données et les systèmes de sécurité cloisonnés créent des zones d'ombre

45

Nombre moyen d'outils de cybersécurité déployés sur les réseaux d'entreprise¹

Les équipes de sécurité doivent être rapides et agiles pour lutter contre les menaces actuelles

92

Nombre de minutes qui s'écoulent avant le déplacement latéral d'une attaque après l'accès initial²

Optimisez la valeur de vos technologies existantes pour réduire les risques

59 %

Pourcentage de responsables sécurité mondiaux affirmant que les données sensibles de leur entreprise ont été compromises au moins une fois au cours de l'année écoulée³

NE VOUS LAISSEZ PAS DUPER PAR DE FAUX XDR

De nombreux fournisseurs vous vendent de prétendus XDR

qui ne seront jamais à la hauteur :

FAUX XDR :

- ✗ NDR ≠ XDR
- ✗ SOAR ≠ XDR
- ✗ SIEM ≠ XDR
- ✗ NDR + SOAR + SIEM ≠ XDR

LE VRAI XDR

DÉTECTION PLUS RAPIDE ET FIABLE

Étendez les technologies de protection aux sources de données tierces pour bénéficier de capacités fiables en matière de détection des menaces, investigation et Threat Hunting, sur toute la surface d'attaque.

ÉCOSYSTÈME DE POINTE

Unifiez la télémétrie pertinente issue de plusieurs technologies et domaines afin d'accélérer la neutralisation des menaces, où qu'elles frappent.

COÛT TOTAL DE POSSESSION RÉDUIT

Optimisez la valeur de votre dispositif de sécurité en garantissant l'intégration de ses composants existants.

INTERVENTION OPTIMISÉE

Permettez aux équipes de sécurité de concevoir et d'automatiser des interventions multi-plateformes en plusieurs étapes, pour une correction chirurgicale couvrant l'ensemble du dispositif de sécurité.

OPÉRATIONS DE SÉCURITÉ PLUS EFFICACES

Mettez intelligemment en corrélation les données de plusieurs sources, rapidement et à grande échelle, afin de fournir des informations de sécurité exploitables à partir d'une console unique.

PRÊT À ADOPTER LE VRAI XDR ?

Évaluez les solutions XDR en suivant cette liste :

- ✓ La solution est-elle dotée de **fonctionnalités natives de détection et d'intervention sur les endpoints** ?
- ✓ Des **informations unifiées sur les menaces** sont-elles fournies pour une détection précise et une intervention optimisée ?
- ✓ La **détection peut-elle être automatisée** au niveau des environnements informatiques, des workloads cloud, du réseau, de la messagerie électronique et des endpoints afin de **réduire le temps de tri** et d'**accélérer l'intervention** ?
- ✓ Des **intégrations cloud** permettent-elles d'assimiler les journaux et les événements issus de plusieurs sources de données et de tiers ?
- ✓ Une **alliance de partenaires stratégiques** a-t-elle été conclue avec des fournisseurs de solutions de pointe ?

« UNE BONNE TECHNOLOGIE XDR REPOSE SUR UNE PLATEFORME EDR PERFORMANTE³. »

— Rapport Forrester « Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR » —

Une solution inégalée pour la détection des menaces, l'investigation, l'intervention et le Threat Hunting, toutes plateformes confondues

FALCON XDR

Protection étendue au-delà de l'endpoint

En savoir plus

SOURCES :
¹ <https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/>
² <https://www.datreading.com/threat-intelligence/attackers-moving-faster-inside-target-networks-report>
³ <https://reprints2.forrester.com/#/assets/2/482/RES116772/report>