



Search. Observe. Protect.

EDR ou XDR

Même si leurs noms semblent similaires, la solution EDR (Endpoint Detection & Response) de protection et de réponse aux points de terminaison et la solution XDR (Extended Detection & Response) de détection et de réponse étendues fournissent des résultats incroyablement différents aux équipes de cybersécurité. Voici une comparaison des avantages dont le personnel peut bénéficier avec chaque solution.

EDR

- Protection ciblée aux points de terminaison
- Utilisation du Machine Learning pour détecter et éviter les malwares et les ransomwares
- Outil autonome doté de fonctionnalités d'intégration minimales
- Aucune maturité de la sécurité avancée requise
- Blocage des attaques au point de terminaison, alertes de détection, isolation des hôtes et réponse automatisée

XDR

- Détection à grande échelle grâce à un ensemble varié d'intégrations au niveau des points de terminaison, du cloud, des utilisateurs, du réseau ou d'autres vecteurs
- Fonctionnalités EDR associées à l'analyse fondée sur le Machine Learning afin de corrélérer les activités et d'identifier les menaces
- Plateforme de sécurité unifiée s'intégrant à d'autres outils qui sert de point de référence unique pour les analystes
- Maturité de la sécurité avancée requise/équipe de sécurité établie
- Fonctionnalités EDR accompagnées d'une exécution et d'une gestion centralisées scalées sur plusieurs solutions, environnements et vecteurs de menaces

Alors qu'EDR peut être tout de suite mis en œuvre dans l'ensemble d'outils existant d'une équipe de sécurité, XDR optimise de manière bien plus efficace la capacité des équipes à monitorer, à détecter et à réagir quelle que soit la surface d'attaque de l'organisation.

Vous vous demandez quelle solution est la plus appropriée pour répondre aux besoins de votre organisation ? Pourquoi ne pas utiliser les deux ? Dans Limitless XDR d'Elastic Security, EDR est un composant fondamental, aux côtés de SIEM et de la sécurité du cloud, de la solution complète. Pour en savoir plus, rendez-vous sur elastic.co/fr/security.