LES PLUS GRANDS AVANTAGES D'XDR

Les solutions XDR reflètent l'évolution continue des produits de cybersécurité. XDR est l'aboutissement de l'évolution des produits de cybersécurité, allant bien au-delà des produits de détection et de réponse aux endpoints (EDR) et des produits de détection et de réponse managés (MDR).

XDR offre une visibilité sur l'ensemble de la surface d'attaque, englobant à la fois les environnements cloud et sur site. Grâce à XDR, les entreprises bénéficient d'une détection et d'une protection améliorées des menaces, en effectuant des déterminations précises en temps réel sur la base de points de données collectés et consolidés sur un éventail de points d'entrée des menaces.

Voici quatre des plus grands avantages de XDR et ce qu'ils signifient pour votre entreprise.

1. Réponse rapide aux incidents

XDR aide les entreprises à identifier les menaces et à y réagir plus rapidement grâce à ses capacités d'analyse avancées.

Ce que cela signifie pour votre entreprise :

- Empêche la propagation des menaces et réduit leur impact
- Réduit le risque de perte de données
- Réduit le risque d'atteinte à la réputation

Mais à quel point XDR est-il plus rapide ? Consultez le tableau ci-dessous pour le découvrir.

Combien de temps faut-il généralement pour résoudre les compromissions ?

	Sans XDR	Avec XDR
Résolution classique des compromissions d'e-mails professionnels (passerelle uniquement)	1 à 2 mois	**1 à 2 heures**
Résolution de l'usurpation d'identité	3 à 4 semaines	**1 à 2 heures**
Résolution des infections par malware	3 à 4 semaines	**Environ 1 heure**
Résolution des menaces internes	3 à 6 mois	**Environ 4 heures**
Résolution des cas d'extorsion sans XDR	Variable	**< 24 heures**

2. Visibilité améliorée sur votre environnement de sécurité

XDR rassemble toutes les données de télémétrie de vos systèmes, qu'il s'agisse de serveurs, de réseaux, du cloud, d'e-mails ou de terminaux, dans une seule interface, ce qui permet de décompartimenter.

Qué significa para su empresa:

- Offre une surveillance complète de la surface d'attaque
- Aide à repérer plus facilement les vulnérabilités ou les erreurs de configuration
- Simplifie la conformité et l'établissement de rapports grâce à des pistes d'audit plus claires

3. Détection des menaces plus intelligente

XDR utilise l'IA, des analyses avancées et des algorithmes d'apprentissage automatique qui lui permettent de repousser les attaques complexes en plusieurs étapes que les outils traditionnels ne détectent souvent pas. Il peut arrêter à la fois les attaques connues et les menaces de type « zero day » inconnues. Il fournit également des informations contextuelles plutôt que des alertes isolées, en détaillant les types d'attaques et les techniques utilisées.

Ce que cela signifie pour votre entreprise :

- Cela vous permet de garder une longueur d'avance sur les tactiques complexes des pirates
- Cela réduit la fatigue liée aux alertes en automatisant la détection
- Cela permet de mieux comprendre les tactiques, techniques et procédures (TTP) des pirates

4. Réduction des coûts de sécurité

Comme la technologie XDR rationalise vos outils et utilise l'automatisation, elle rend vos activités de sécurité plus efficaces et moins coûteuses.

Ce que cela signifie pour votre entreprise :

- Réduction de la duplication des paiements pour les outils de sécurité
- Vous disposez donc d'un budget plus conséquent pour investir ailleurs
- Le retour sur investissement en matière de sécurité est maximisé

Ce ne sont en aucun cas les seuls bénéfices de XDR. Pour en savoir plus sur les bénéfices XDR et comment cela fonctionne, téléchargez notre ebook XDR : XDR, une approche stratégique de la gestion des menaces.

Barracuda