Optimisation des détections

Publié: 2024-07-18

Voici quelques bonnes pratiques à mettre en œuvre pour améliorer vos détections : ajoutez des informations sur votre réseau, activez le système ExtraHop pour détecter le trafic potentiellement suspect et filtrez les pages affichées en fonction de vos priorités.

La plupart de ces paramètres fournissent un contexte sur votre réseau que vous pouvez fournir pour améliorer à la fois l'apprentissage automatique et les détections basées sur des règles. Ces paramètres sont parfois négligés et peuvent affecter la qualité de vos détections.

Configurer le déchiffrement

Le trafic HTTP chiffré est un vecteur courant d'attaques, en partie parce que les attaquants savent que le trafic est généralement masqué. Et si votre réseau est doté d'Active Directory, un certain nombre de détections sont masquées dans le trafic chiffré sur le domaine.

Nous vous recommandons vivement d'activer le déchiffrement pour SSL/TLS et Active Directory.

Configuration des paramètres de réglage

Ce paramètre améliore la précision des détections basées sur des règles. Vous fournir des détails au système ExtraHop sur votre environnement réseau afin de fournir un contexte sur les appareils observés.

Par exemple, une détection basée sur des règles est générée lorsqu'un équipement interne communique avec des bases de données externes. Si un trafic vers une base de données externe est attendu ou si la base de données fait partie d'une infrastructure de stockage ou de production légitime basée sur le cloud, vous pouvez définir un paramètre de réglage pour ignorer le trafic vers la base de données externe approuvée.

Configurer les localités du réseau

Ce réglage vous permet de classer interne ou externe des terminaux auxquels vous faites confiance, tels qu'un bloc CIDR d'adresses IP auquel vos appareils se connectent régulièrement. Les détections par apprentissage automatique et les mesures du système reposent sur la classification des équipements et du trafic .

Par exemple, si vos appareils se connectent régulièrement à un domaine inconnu mais fiable classé comme adresse IP externe, les détections sont supprimées pour ce domaine.

Création de règles d'exceptions

Ces paramètres vous permettent de masquer les détections une fois que le système les a générés. Si vous constatez une détection qui n'apporte aucune valeur ajoutée, vous pouvez réduire le bruit de votre vue d'ensemble.

Par exemple, si une détection est générée à partir d'un délinquant, d'une victime ou d'autres critères qui ne sont pas préoccupants pour votre réseau, vous pouvez masquer toutes les détections passées et futures utilisant ces critères.

Partagez des données externes en texte brut

Cette option permet au service d'apprentissage automatique de collecter des adresses IP, des noms d'hôtes et des domaines qui sont associés à des activités suspectes.

En activant cette option, vous ajoutez à un ensemble de données collectif de menaces potentielles qui peuvent vous aider et contribuer à la communauté de la sécurité.

Détections de traces

Cette option vous permet de attribuer une détection à un utilisateur, ajouter des notes et mettre à jour le statut de reconnu à fermé. Vous pouvez ensuite filtrer la page Détections pour effacer les problèmes résolus ou vérifier les détections.