Optimiser les détections

Publié: 2023-09-19

Voici quelques bonnes pratiques à mettre en œuvre pour améliorer vos détections : ajoutez des détails sur votre réseau, activez le système ExtraHop pour voir le trafic potentiellement suspect et filtrez l'affichage de votre page en fonction de vos priorités.

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

Configurer le décryptage

Le trafic HTTP chiffré est un vecteur courant d'attaques, en partie parce que les attaquants savent que ce trafic est généralement caché. Et si votre réseau dispose d'Active Directory, un certain nombre de détections sont cachées dans le trafic crypté à travers le domaine.

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

Configurer les paramètres de réglage

Ce paramètre améliore la précision des détections basées sur des règles.

Par exemple, une détection basée sur des règles est générée lorsqu'un périphérique interne communique avec des bases de données externes. Si le 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 paramètre vous permet de classer les points de terminaison internes ou externes et les domaines auxquels vous faites confiance, tels qu'un domaine de confiance auquel vos appareils se connectent régulièrement.

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

.

Régler les détections

Ces paramètres vous permettent de masquer ou de supprimer des détections après que le système les a générées. Si vous voyez une détection qui n'apporte pas de valeur ajoutée, vous pouvez réduire le bruit dans votre vue d'ensemble.

Par exemple, si une détection est générée avec un auteur, une victime ou un autre critère qui ne concerne pas votre réseau, vous pouvez masquer toutes les détections passées et futures avec ce critère.

Partager des données externes en clair

Cette option permet au service d'apprentissage automatique de collecter les adresses IP, les noms d'hôte et les domaines associés à des activités suspectes

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

.

Suivi des détections

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