Analyse collective des menaces FAQ

Publié: 2023-09-19

Qu'est-ce que l'analyse collective des menaces ?

L'analyse collective des menaces permet aux utilisateurs de partager certaines données avec ExtraHop afin d'améliorer la précision des détections, telles que le balisage de commande et de contrôle (C&C).

Par défaut, toutes les données envoyées au service ExtraHop Cloud qui pourraient identifier de manière unique un participant au réseau (comme une adresse IP ou un nom d'utilisateur) sont cryptées avec une clé stockée sur le capteur et à laquelle ExtraHop n'a pas accès.

Les utilisateurs de Reveal(x) Enterprise peuvent envoyer des données au Service d'apprentissage automatique en activant les Services cloud ExtraHop dans les paramètres d'administration. Par exemple, le système peut envoyer des adresses IP, des noms de domaine et des noms d'hôte externes en clair qui sont associés à un comportement suspect détecté. Ce paramètre est activé par défaut dans Reveal(x)360 et ne peut pas être désactivé. Pour obtenir une liste complète des types de données envoyées au service d'apprentissage automatique ExtraHop et voir comment les données sont utilisées pour améliorer la détection des menaces, consultez la section Apprentissage automatique de la vue d'ensemble de la sécurité, de la confidentialité et de la confiance d'ExtraHop.

En acceptant de partager ces données en clair, vous contribuez à un vaste ensemble de données communautaires qui peuvent être analysées pour le bénéfice de tous, en particulier le vôtre. Cet ensemble de données comprend à la fois des données en clair et des métadonnées dépersonnalisées associées aux menaces détectées par ExtraHop.

Dans quelle mesure mes données sont-elles sécurisées ?

Lorsque vous choisissez d'envoyer à ExtraHop les adresses IP, les noms d'hôte et les noms de domaine externes en clair observés sur votre réseau, le capteur ExtraHop envoie ces métadonnées au service d'apprentissage automatique par le biais de connexions TLS 1.2 ou TLS 1.3 et d'une confidentialité parfaite (PFS). Les données en transit et les données au repos sont stockées en toute sécurité dans un entrepôt de données crypté et hautement protégé.

Pour en savoir plus sur la façon dont ExtraHop sécurise vos données, consultez la page ExtraHop Security, Privacy, and Trust Overview (Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop).

Pourquoi devrais-je m'inscrire ?

Voici les avantages que vous pouvez tirer de votre contribution à la recherche et à l'analyse collectives.

Améliorer le contexte de vos détections

L'apprentissage automatique basé sur le cloud d'ExtraHop peut tirer parti des données en clair lors de l'analyse des comportements suspects. Les données riches font apparaître des détections plus fiables.

Prenons l'exemple du site Web d'un café local dont les analyses Web sont mal configurées. Le trafic du site web peut être détecté sur votre réseau pour un balisage rapide de 30 secondes, un comportement qui est également couramment observé dans les balises de commande et de contrôle (C&C) malveillantes. Cependant, en ayant accès au nom d'hôte et à l'adresse IP en clair du serveur d'analyse associé à la détection, le système ExtraHop peut mieux déterminer si le balisage rapide est lié à une source malveillante connue. Un meilleur contexte permet à ExtraHop de vous indiquer quand le trafic est malveillant et de réduire le nombre de faux positifs

.

Aidez à stopper les nouvelles attaques sur votre réseau

ExtraHop effectue des analyses de big data pour repérer les attaques furtives et avancées que les organisations individuelles pourraient négliger.

Par exemple, ExtraHop peut observer que des appareils sur plusieurs réseaux établissent des tunnels SSH inversés vers une adresse IP suspecte. Après une analyse plus approfondie, l'adresse IP suspecte semble héberger un serveur C&C qui présente des comportements précédemment associés à un groupe de menaces connu. ExtraHop met immédiatement à jour tous les capteurs déployés avec les détections afin de protéger tous les déploiements connectés au cloud contre la nouvelle menace identifiée.

Améliorer les modèles d'apprentissage automatique dans vos détections

ExtraHop exploite les données fournies par la communauté lors de l'entraînement des algorithmes d'apprentissage automatique et du développement de nouveaux modèles d'apprentissage automatique, qui sont conçus pour détecter les attaques sur les réseaux d'utilisateurs. Nous affinons également notre compréhension des modèles de comportement bénin en surveillant la façon dont les comportements se manifestent sur les réseaux de différents secteurs, tailles et emplacements géographiques.

Puis-je me désengager ?

Dans les capteurs Reveal(x) Enterprise, vous pouvez désactiver le paramètre par défaut qui active l'analyse collective des menaces.

Les détecteurs qui prennent en charge l'analyse collective des menaces affichent une notification de rappel à tous les utilisateurs dans les vues Groupe par type de détection et Détail de la détection. Les administrateurs peuvent choisir de masquer les rappels dans le produit.

Les paramètres suivants sont disponibles :

- Fournir des adresses IP externes, des noms de domaine et des noms d'hôte pour l'analyse collective des menaces.
- Ne pas contribuer à l'analyse collective des menaces
- Ne pas contribuer à l'analyse collective des menaces et ne pas afficher les rappels dans le produit.