FAQ sur l'analyse collective des menaces

Publié: 2024-04-10

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 Command-and-Control (C&C), et de générer de nouvelles détections, telles que l'identification de hachages de fichiers malveillants.

Par défaut, toutes les données envoyées au service ExtraHop Cloud susceptibles d' identifier de manière unique un participant au réseau (comme une adresse IP ou un nom d'utilisateur) sont cryptées à l'aide d'une clé stockée sur le sonde et auxquels 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 et en optant pour l'analyse collective des menaces dans les paramètres d' administration. Par exemple, le système peut envoyer des noms de domaine, des noms d'hôtes, des hachages de fichiers et des adresses IP externes. Ce paramètre est activé par défaut dans Reveal (x) 360 et ne peut pas être désactivé. Pour obtenir la liste complète des types de données envoyés au service d'apprentissage automatique ExtraHop et pour voir comment les données sont utilisées pour améliorer la détection des menaces, consultez la section Machine Learning du Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop.

En choisissant de partager ces données en texte brut, vous contribuez à un vaste ensemble de données communautaire qui peut être analysé dans l'intérêt de tous, en particulier du vôtre. Cet ensemble de données comprend à la fois des données en texte brut et des métadonnées anonymisées associées aux menaces détectées par ExtraHop.

Dans quelle mesure mes données sont-elles sécurisées ?

Quand tu optez pour l'analyse collective des menaces la sonde ExtraHop envoie ces métadonnées au service d'apprentissage automatique via des connexions TLS 1.2 ou TLS 1.3 et une confidentialité parfaite (PFS). Les données en transit et les données au repos sont stockées en toute sécurité dans une banque de données cryptée hautement protégée.

Vous pouvez en savoir plus sur la manière dont ExtraHop sécurise vos données dans le 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.

Améliorez le contexte de vos détections

L'apprentissage automatique basé sur le cloud ExtraHop peut tirer parti des données en texte brut pour analyser les comportements suspects. Des données riches font apparaître des détections avec une plus grande fiabilité.

Prenons l'exemple du site Web d'un café local dont les analyses Web sont mal configurées. Ce site Web contacte fréquemment un serveur d'analyse externe pour obtenir des statistiques de performance. Le trafic du site Web peut être détecté sur votre réseau lors d'un balisage rapide de 30 secondes, un comportement également fréquemment observé dans les balises de commande et de contrôle (C&C) malveillantes. Cependant, en accédant au nom d'hôte externe en texte brut et à l'adresse IP 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. L'amélioration du 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 données volumineuses pour détecter les attaques furtives et avancées que les organisations pourraient ignorer. L'ensemble de la clientèle est automatiquement et immédiatement protégé contre chaque nouvelle menace identifiée.

Par exemple, ExtraHop peut observer que des appareils de 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 équipements déployés capteurs avec des détections pour protéger tous les déploiements connectés au cloud contre la nouvelle menace identifiée.

Améliorez les modèles d'apprentissage automatique dans vos détections

ExtraHop exploite les données provenant de la communauté pour entraîner des algorithmes d'apprentissage automatique et développer de nouveaux modèles d'apprentissage automatique, conçus pour détecter les attaques sur les réseaux des utilisateurs. Nous affinons également notre compréhension des comportements bénins en surveillant la façon dont les comportements se manifestent sur les réseaux de différents secteurs, tailles et zones géographiques.

Quelle est la différence entre des renseignements sur les menaces étendus et une analyse collective des menaces ?

Les données envoyées à l'analyse collective des menaces sont ajoutées à un pool de données anonymisées et étudiées pour améliorer les détections par apprentissage automatique, identifier de nouveaux types d'attaques, générer des détections pour les hachages de fichiers malveillants et améliorer la précision des détections existantes. Données partagées avec renseignements sur les menaces élargis est immédiatement examiné par rapport à une collection étendue de renseignements sur les menaces, puis est rejeté.

Les deux services sont activés automatiquement dans Reveal (x) 360, mais les administrateurs de Reveal (x) Enterprise doivent s'inscrire dans les paramètres d'administration.

Puis-je me désinscrire ?

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

Les détecteurs qui prennent en charge l'analyse collective des menaces affichent à tous les utilisateurs une notification de rappel dans la vue Grouper par type de détection et la vue détaillée de la détection. Les administrateurs peuvent choisir de masquer les rappels intégrés au produit.

Les paramètres suivants sont disponibles :

- Ajoutez des noms de domaine, des noms d'hôte, des hachages de fichiers et des adresses IP externes pour une analyse collective des menaces
- Ne contribuez pas à l'analyse collective des menaces
- Ne contribuez pas à l'analyse collective des menaces et n'affichez pas de rappels intégrés au produit