FAQ étendue sur les renseignements sur les menaces

Publié: 2024-04-10

Qu'est-ce que les renseignements sur les menaces étendus ?

Les renseignements étendus sur les menaces permettent aux utilisateurs de partager certaines données avec ExtraHop pour les comparer à une collection plus importante d'indicateurs de renseignements sur les menaces CrowdStrike, de points de terminaison bénins et d'autres informations sur le trafic réseau. L'analyse des données par rapport à une bibliothèque étendue de renseignements permet de mieux identifier les terminaux malveillants, d'améliorer la précision des détections et d'enrichir contextuellement les informations de détection afin de permettre des évaluations rapides et éclairées des détections.

Les utilisateurs de Reveal (x) Enterprise doivent activer ce service en activant les services cloud ExtraHop et en optant pour des renseignements sur les menaces étendus dans les paramètres d'administration . Une fois activé, le système peut envoyer les adresses IP, les noms de domaine, les noms d'hôte, les hachages de fichiers et les URL observées sur votre système pour un examen en temps réel par rapport à une plus grande collection de renseignements sur les menaces. 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 à ExtraHop Cloud Services et pour voir comment les données sont utilisées pour améliorer la détection des menaces, consultez la section Machine Learning du.

Dans quelle mesure mes données sont-elles sécurisées ?

Quand tu Adhérez à des renseignements sur les menaces étendus, la sonde ExtraHop envoie ces métadonnées à ExtraHop Cloud Services via des connexions TLS 1.2 ou TLS 1.3 et une confidentialité parfaite (PFS). Les adresses IP, les noms de domaine, les noms d'hôte, les hachages de fichiers et les URL envoyés aux services cloud pour des renseignements sur les menaces étendus sont immédiatement examinés puis supprimés.

Vous pouvez en savoir plus sur la manière dont ExtraHop sécurise vos données dans Présentation de la sécurité, de la confidentialité et de la confiance d'ExtraHop.

Pourquoi devrais-je m'inscrire ?

Voici comment vous pouvez tirer parti de renseignements sur les menaces étendus.

La puissance du traitement dans le cloud

L'apprentissage automatique basé sur le cloud ExtraHop offre des capacités de traitement qui vont bien au-delà de la capacité des capteurs individuels. En optant pour des renseignements sur les menaces étendus, vous pouvez accéder à une vaste bibliothèque d'indicateurs de menaces qui ne pourraient pas être appliqués efficacement au niveau des sondes, mais qui peuvent être traités en temps réel grâce à la puissance informatique des ressources cloud d'ExtraHop.

Couverture CrowdStrike supplémentaire

Le système ExtraHop propose des collections de menaces de qualité provenant de CrowdStrike en tant que composant standard des renseignements sur les menaces intégrés. En raison de contraintes de traitement, une grande partie de l'intelligence de CrowdStrike ne peut pas être incluse dans les capteurs. En optant pour des renseignements sur les menaces étendus, vous bénéficiez de la puissance de traitement supplémentaire fournie par ExtraHop Cloud Services et vous permet de disposer d'un ensemble beaucoup plus important d'indicateurs CrowdStrike à comparer au trafic de votre réseau.

Plus d'informations maintenant, moins d'investigations plus tard

Le renseignement sur les menaces ne consiste pas uniquement à identifier les adresses IP suspectes ou les hachages de fichiers malveillants. Il s'agit également d'identifier rapidement le trafic qui n'est pas suspect. ExtraHop exploite les données réseau pour classer les activités réseau bénignes et

© 2024ExtraHop Networks, Inc. Tous droits réservés.

éliminer le bruit des activités inoffensives des flux de travail d'investigation . Le fait d'opter pour des renseignements sur les menaces étendus permet à ExtraHop de filtrer ce que les analystes vont voir grâce à la plus grande collection possible d'indicateurs de menaces et de modèles de comportement bénins, et de ne présenter que des informations exploitables de qualité.

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

Données envoyées à analyse collective des menaces est ajouté à un pool de données anonymisé et étudié 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. Les données partagées dans le cadre de renseignements sur les menaces étendus sont immédiatement examinées par rapport à une collection étendue de renseignements sur les menaces, puis sont supprimées.

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 ?

Ce service est activé dans Reveal (x) 360 par défaut et ne peut pas être désactivé. Les systèmes Reveal (x) Enterprise sont désactivés par défaut des renseignements sur les menaces étendus et peuvent accéder au service dans les paramètres d'administration.

Les paramètres suivants sont disponibles :

- J'accepte d'envoyer des adresses IP, des noms de domaine, des noms d'hôtes, des hachages de fichiers et des URL à ExtraHop Cloud Services.
- Je ne souhaite pas envoyer d'adresses IP, de noms de domaine, de noms d'hôte, de hachages de fichiers et d'URL à ExtraHop Cloud Services et je comprends que mes données ne seront pas examinées par rapport à la collecte complète de renseignements sur les menaces.

La désinscription mettra-t-elle fin à toutes les détections basées sur les renseignements sur les menaces ?

Non Le fait de ne pas recevoir de renseignements sur les menaces étendus ne fera qu'empêcher l' examen de vos données par rapport à une collecte complète de renseignements sur les menaces. Les données du réseau seront toujours examinées par rapport aux renseignements sur les menaces provenant de sources locales, notamment les collections de menaces intégrées, les fichiers STIX téléchargés et les flux TAXII. Par exemple, vous verrez toujours des détections basées sur les collections de menaces intégrées à CrowdStrike.