FAQ sur les détections

Publié: 2023-11-14

Voici quelques réponses aux questions fréquemment posées sur les détections.

En quoi les détections diffèrent-elles des alertes ?

Alertes et les détections sont similaires dans la mesure où elles fournissent toutes deux des informations sur l'état de votre réseau. Le tableau suivant décrit leurs différences. Les alertes fournissent Les conditions d'alerte configurées déterminent le moment où une alerte est générée.

	Alertes	Détections
Comment sont-ils générés ?	Par conditions que vous définissez dans les paramètres d'alerte. Vous pouvez configurer des alertes de tendance ou de seuil.	Observé automatiquement à partir des données de votre réseau par le service d'apprentissage automatique ExtraHop.
Comment puis-je les consulter ?	Cliquez **Alertes** depuis le menu supérieur du système ExtraHop.	Cliquez **Détections** depuis le menu supérieur du système ExtraHop.
Comment configurer les notifications par e-mail ?	Tu peux ajouter une notification à une configuration d'alerte pour envoyer des e-mails lorsque les conditions d'alerte sont remplies.	Tu peux créer une règle de notification pour envoyer des e-mails concernant les détections répondant à des critères spécifiques.
Quels sont les avantages ?	Vous décidez quels appareils et services prioritaires surveiller et déterminez le niveau de modification qui génère des notifications.	Les modifications notables apportées au comportement de votre réseau sont automatiquement mises en évidence. En fournissant des informations sur les détections, vous aidez l'algorithme du Service d'apprentissage automatique à mieux comprendre votre réseau.

Qu'est-ce qu'un indice de risque ? (ExtraHop Reveal (x) uniquement)

UN indice de risque indique la gravité d'une détection et est calculé en fonction de la probabilité d'une attaque, de la difficulté d' exploiter la détection et du niveau d'impact sur vos opérations.

Les scores de risque sont regroupés selon l'un des niveaux de gravité codés par couleur suivants :

- Rouge = 80-99
- Orange = 31-79
- Jaune = 1-30

Aucun indice de risque n'est affiché pour une détection individuelle si aucun score n'a été évalué et défini pour cette détection.

Pourquoi ne puis-je pas afficher les détails de l'équipement source lors d'une détection ?

Si la source d'une détection est un équipement qui n'a pas été découvert par le système ExtraHop, la détection affiche uniquement l'adresse IP et le nom d'hôte de l'équipement, s'ils sont disponibles. Vous pouvez survoler l'équipement non découvert pour voir la géolocalisation de l'adresse IP et un lien vers le site Web ARIN Whois.

Depuis combien de temps les détections sont-elles détectées ?

Les détections par apprentissage automatique sont identifiées il y a une semaine après la connexion du service. Le service identifie ensuite toutes les nouvelles détections à venir.

Notez que le service d'apprentissage automatique a besoin de quatre semaines (28 jours) de données pour calculer une plage attendue de valeurs métriques. La plage attendue représente le comportement normal du réseau. Le traitement des données est généralement terminé en quelques heures.

Puis-je me connecter au service d'apprentissage automatique via un proxy ?

Le service d'apprentissage automatique prend en charge les proxys implicites et explicites. Le proxy nécessite que le DNS résolve tous les domaines*.extrahop.com, et le port 443 sortant est ouvert à toutes les adresses IP sur Internet. Ces paramètres sont implémentés sur le pare-feu pour l'adresse IP source du proxy.

Pour plus d'informations sur la configuration d'un proxy explicite, voir Connectez-vous aux services cloud ExtraHop via un proxy.

Quelles données sont envoyées du système ExtraHop au service d'apprentissage automatique ?

Le service d'apprentissage automatique tire parti des capacités de traitement uniques du système ExtraHop pour « prétraiter » les données filaires pour des centaines de métriques sur site. Le système ExtraHop chiffre les valeurs métriques et les adresses IP envoyées au service d'apprentissage automatique. Le système ExtraHop n'envoie pas de métriques personnalisées ni de données sensibles telles que des noms de fichiers, des chaînes ou des charges utiles.

Dans quelle mesure les détections sont-elles sécurisées ?

Les détections sont conçues pour être sécurisées de bout en bout. Contrairement à une solution SaaS classique, les détections n'ingèrent pas les charges utiles, les noms de fichiers, les chaînes ou les autres catégories de données susceptibles de contenir des informations sensibles. Le service d'apprentissage automatique ExtraHop a reçu la certification de conformité SOC 2, type 1.

Comment ajouter une licence nouvelle ou mise à jour pour le service d'apprentissage automatique à mon système ExtraHop ?

Si vous avez acheté un nouveau système ExtraHop qui inclut une licence pour le service d'apprentissage automatique, vous recevrez un e-mail contenant une nouvelle clé de produit. Suivez les instructions pour enregistrez votre appareil.

Si vous avez ajouté une licence pour le service d'apprentissage automatique, votre licence mise à jour est automatiquement ajoutée à votre système ExtraHop, mais elle doit tout de même être appliquée. Suivez les instructions pour appliquer une licence mise à jour.

Pourquoi ne reçois-je pas certaines détections de machine learning ?

Le service d'apprentissage automatique prend en charge les versions du micrologiciel ExtraHop pendant environ 15 mois après la publication du micrologiciel. Si vous ne mettez pas à jour votre firmware ExtraHop pendant plus de 15 mois, il est possible que vous ne receviez pas les dernières mises à jour et les nouvelles détections du service d'apprentissage automatique. Contactez le support ExtraHop pour obtenir de l'aide concernant la mise à niveau du firmware en création d'un dossier sur le portail client (connexion requise).

Une fois ma licence du service d'apprentissage automatique expirée, puis-je toujours consulter mes détections précédentes ?

Oui, les détections précédentes restent disponibles dans votre système ExtraHop.