Priorités d'analyse

Publié: 2025-02-12

Le système ExtraHop analyse le trafic et collecte les données de tous les appareils découverts sur un seul sonde. Chaque équipement découvert reçoit un niveau d'analyse qui détermine quelles données et mesures sont collectées pour un équipement. Les priorités d'analyse déterminent le niveau d'analyse reçu par un équipement.

Important: Les priorités d'analyse peuvent être géré de manière centralisée depuis une console.

Vidéos Consultez la formation associée : Priorités d'analyse

Niveaux d'analyse

Le système ExtraHop analyse intelligemment les appareils et attribue automatiquement un niveau d'analyse. Vous pouvez également configurer le niveau d'analyse pour les appareils et les groupes d'appareils.

Note: Les enregistrements et les paquets sont disponibles pour tous les périphériques des systèmes ExtraHop configurés avec un espace de stockage des enregistrements ou un magasin de paquets, quel que soit le niveau d'analyse.

Chaque équipement reçoit l'un des niveaux d'analyse suivants.

mode de découverte

Le système ExtraHop identifie le matériel et les logiciels connus des équipements, les utilisateurs authentifiés et les adresses IP attribuées et associées. Le système ExtraHop génère également des détections et des graphiques qui montrent l'activité du protocole observée sur l'équipement. Tous les appareils reçoivent un minimum de ce niveau d'analyse, à l'exception des appareils parents L2.

Analyse standard

Le système ExtraHop inclut au moins une semaine de données métriques et de relations entre pairs L2-L3 que vous pouvez explorer instantanément grâce à des détections, des graphiques et des cartes d'activité. Le système ExtraHop identifie également le matériel et les logiciels connus des équipements, les utilisateurs authentifiés et les adresses IP attribuées et associées. Apprenez comment prioriser les groupes pour l'analyse standard.

Analyse avancée

Le système ExtraHop inclut au moins une semaine de métriques L2-L7 issues de plus de 50 protocoles et de données sur les relations entre pairs que vous pouvez explorer instantanément grâce à des détections, des graphiques et des cartes d'activité, ainsi que des tableaux de bord, des rapports et des alertes personnalisés. Le système ExtraHop identifie également le matériel et les logiciels connus des équipements, les utilisateurs authentifiés et les adresses IP attribuées et associées. Apprenez comment prioriser les groupes pour l'Analyse avancée ou ajouter un équipement individuel à une liste de surveillance.

Analyse des parents L2

L'analyse des parents L2 n'est applicable que si L3 Discovery est activée sur le système ExtraHop. À l'exception des passerelles et des routeurs, les appareils parents L2 reçoivent automatiquement ce niveau d'analyse, qui collecte les métriques du protocole L2-L3 et les cartes d'activité.

Analyse des flux

Un flux sonde collecte des données à partir de journaux de flux, au lieu de paquets, pour analyse par le système ExtraHop. Appareils découverts sur le flux capteurs reçoivent automatiquement ce niveau d'analyse. Les paramètres du système Analysis Priorities ne sont pas disponibles pour le flux capteurs, et les appareils de Flow Analysis ne peuvent pas être ajoutés à la liste de surveillance.

Voir un tableau qui compare ces niveaux d'analyse.

Prioriser les appareils et les groupes

Vous pouvez ajouter la plupart des appareils à une liste de surveillance pour garantir une analyse avancée ou vous pouvez ajouter des groupes d'appareils à une liste ordonnée qui classe les appareils par ordre de priorité pour l'Analyse avancée et l'Analyse standard.

Voici quelques considérations importantes concernant la hiérarchisation des appareils dans la liste de surveillance :

- Les appareils restent sur la liste de surveillance même lorsqu'ils sont inactifs, mais les statistiques ne sont pas collectées pour les appareils inactifs. Même lorsqu'ils sont inactifs, les appareils de liste de surveillance continuent de faire partie de votre capacité d' analyse avancée.
- Le nombre d'appareils figurant dans la liste de surveillance ne peut pas dépasser votre capacité d'Analyse avancée.
- Les appareils ne peuvent être ajoutés à la liste de surveillance que depuis la page des propriétés de l'appareil ou la page de liste des appareils. Vous ne pouvez pas ajouter d'appareils à la liste de surveillance depuis la page Priorités d'analyse.
- Si vous souhaitez ajouter plusieurs appareils à la liste de surveillance, nous vous recommandons de créer un groupe dproximatifs d'équipements et puis donner la priorité à ce groupe pour l'analyse avancée.
- Les appareils recevant une analyse parentale L2 ou une analyse de flux ne peuvent pas être ajoutés à la liste de surveillance.

Voici quelques considérations importantes concernant la hiérarchisation des groupes d'équipements :

- Classez les groupes d'équipements de la priorité la plus élevée à la plus faible de la liste.
- Cliquez et faites glisser les groupes pour modifier leur ordre dans la liste.

Par défaut, le système ExtraHop remplit intelligemment les niveaux d'analyse avancée et standard au maximum de sa capacité. Voici quelques considérations importantes concernant les niveaux de capacité et l'option de remplissage automatique :

- Les appareils classés par ordre de priorité dans la liste de surveillance ou par le biais d'un groupe hiérarchisé répondent d'abord aux niveaux d' analyse les plus élevés, puis en fonction des appareils découverts le plus tôt.
- Les appareils sont automatiquement classés par ordre de priorité pour l'Analyse avancée par le système si l'équipement est associé à certaines détections, s'il a accepté ou initié une connexion externe, ou s'il exécute des outils d'attaque courants.
- Les propriétés de l'appareil telles que le rôle, le matériel et les logiciels, l'activité du protocole et l'historique des détections peuvent également déterminer les niveaux d'analyse.
- L'option Remplir automatiquement est activée par défaut. Si cette option est désactivée, tous les appareils qui ne figurent pas dans les groupes prioritaires ou dans la liste de surveillance sont supprimés et le système ExtraHop définit la priorité pour chaque équipement.
- Votre abonnement et votre licence ExtraHop déterminent les niveaux de capacité maximum.

Consultez les FAQ sur les priorités d'analyse pour en savoir plus sur les capacités des niveaux d'analyse et l'ordre de priorité.

Comparez les niveaux d'analyse

Niveau d'analyse	Fonctionnalités	Comment recevoir ce niveau
mode de découverte	• Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés	Les appareils reçoivent automatiquement le mode de découverte s'ils ne sont pas en mode Standard, Advanced ou L2 Parent Analysis.

Niveau d'analyse	Fonctionnalités	Comment recevoir ce niveau
	• Logiciel • Marque et modèle du matériel	
Analyse standard	• Métriques L2-L3 • Cartes d'activités • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	Hiérarchiser les groupes d'équipements pour l'analyse standard.
Analyse avancée	• Métriques L2-L7 • Métriques personnalisées • Cartes d'activités • Détections • Protocoles observés • Adresses IP • Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	Hiérarchiser les groupes d'équipements pour l'Analyse avancée ou ajouter des appareils individuels à la liste de surveillance.
Analyse des parents L2 (Applicable uniquement si L3 Discovery est activé)	• Métriques L2-L3 • Cartes d'activités	Les appareils parents L2 reçoivent automatiquement une analyse parent L2, à l'exception des passerelles et des routeurs.
Analyse des flux	• Métriques L2-L3 • Cartes d'activités • Protocoles observés • Adresse IP • Propriétés de l'instance cloud • Types de détection limités	Les appareils reçoivent automatiquement une analyse de flux s'ils sont découverts sur un capteur de débit.