Priorités d'analyse

Publié: 2024-11-03

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

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

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

mode de découverte

Le système ExtraHop identifie le matériel et les logiciels connus de l'équipement, 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 L2-L3 et de relations avec les pairs que vous pouvez explorer instantanément à l'aide de détections, de graphiques et de cartes d'activité. Le système ExtraHop identifie également le matériel et les logiciels connus de l'équipement, les utilisateurs authentifiés et les adresses IP attribuées et associées. Apprenez comment hiérarchiser les groupes pour l'analyse standard.

Analyse avancée

Le système ExtraHop inclut au moins une semaine de métriques L2-L7 provenant de plus de 50 protocoles et de données sur les relations avec les pairs que vous pouvez explorer instantanément via 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 de l'équipement, les utilisateurs authentifiés et les adresses IP attribuées et associées. Apprenez comment hiérarchiser les groupes pour l'Analyse avancée ou ajouter un équipement individuel à une liste de surveillance.

Analyse des parents L2

L2 Parent Analysis n'est applicable que si L3 Discovery est activé 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, plutôt que de paquets, pour analyse par le système ExtraHop. Appareils découverts lors du flux capteurs recevez automatiquement ce niveau d'analyse. Les paramètres système des priorités d'analyse ne sont pas disponibles pour le flux capteurs, et les appareils de Flow Analysis ne peuvent pas être ajoutés à la liste de surveillance.

Consultez un tableau qui compare ces niveaux d'analyse.

Hiérarchisation des appareils et des groupes

Le système ExtraHop peut analyser des centaines de milliers d'appareils et déterminer automatiquement le niveau d'analyse que chaque équipement reçoit, mais vous pouvez contrôler quels appareils sont priorisés pour l'analyse avancée et standard.

La plupart des appareils peuvent être ajoutés à une liste de surveillance pour garantir une analyse avancée ou vous pouvez ajouter des groupes d'équipements à une liste ordonnée afin de les classer par ordre de priorité pour l'analyse avancée et l'analyse standard.

Voici quelques points importants à prendre en compte pour hiérarchiser les appareils dans la liste de surveillance :

- Les appareils restent sur la liste de surveillance même lorsqu'ils sont inactifs, mais aucune statistique n'est collectée pour les appareils inactifs.
- 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 qu'à partir de la page des propriétés de l'équipement ou de la page de liste des équipements. Vous ne pouvez pas ajouter d'appareils à la liste de surveillance depuis la page des priorités d'analyse.
- Si vous souhaitez ajouter plusieurs appareils à la liste de surveillance, nous vous recommandons créer un groupe d'équipements puis prioriser ce groupe pour l' analyse avancée.
- Les appareils recevant une analyse parent 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 dans la liste.
- Cliquez et faites glisser les groupes pour modifier leur ordre dans la liste.
- Assurez-vous que chaque équipement du groupe est actif ; les groupes contenant un grand nombre d' appareils occupent de la capacité et les appareils inactifs ne génèrent pas de mesures.
- Vous ne pouvez pas hiérarchiser plus de 200 groupes d'équipements pour chaque niveau.

Par défaut, le système ExtraHop remplit automatiquement les niveaux d'analyse avancée et standard jusqu'à sa capacité maximale. 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 via un groupe hiérarchisé remplissent d'abord les niveaux d' analyse les plus élevés, puis les appareils découverts le plus tôt.
- Les appareils sont priorisés pour l'Analyse avancée s'ils sont associés à certaines détections, s'ils ont accepté ou initié une connexion externe, ou s'ils exécutent des outils d'attaque courants.
- Les propriétés de l'appareil, telles que le rôle, le matériel et le logiciel, l'activité du protocole, l'historique de détection et la valeur élevée, peuvent également déterminer les niveaux d'analyse.
- L'option Remplissage automatique 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 de chaque équipement.
- Votre abonnement et votre licence ExtraHop déterminent les niveaux de capacité maximaux.

Voir le FAQ sur les priorités d'analyse pour en savoir plus sur les capacités des niveaux d'analyse.

Comparez les niveaux d'analyse

Niveau d'analyse	Fonctionnalités	Comment recevoir ce niveau
mode de découverte	• Détections • Protocoles observés • Adresses IP	Les appareils reçoivent automatiquement le mode de découverte s'ils ne sont pas en

Niveau d'analyse	Fonctionnalités	Comment recevoir ce niveau
	• Utilisateurs authentifiés • Logiciel • Marque et modèle du matériel	mode Standard, Advanced ou L2 Parent Analysis.
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.