Aperçu de la sécurité

Publié: 2024-04-10

L'aperçu de la sécurité affiche plusieurs graphiques qui mettent en évidence les données sous différents angles concernant les détections. Ces graphiques peuvent vous aider à évaluer l'étendue des risques de sécurité, à lancer des enquêtes sur des activités inhabituelles et à atténuer les menaces de sécurité. Les détections sont analysées toutes les 30 secondes ou toutes les heures, selon la métrique.

Vidéos Consultez la formation associée : Présentation de la sécurité, du réseau et du périmètre

Recommandé pour le triage

Ce graphique présente une liste des détections recommandées par ExtraHop sur la base d'une analyse contextuelle de votre environnement. Cliquez sur une détection pour afficher carte de détection dans Vue de triage sur la page Détections.

Enquêtes

Ce graphique fournit un décompte des enquêtes créées au cours de l' intervalle de temps sélectionné. Le décompte inclut les enquêtes recommandées par ExtraHop ou créées par les utilisateurs. Cliquez sur le graphique pour afficher tableau des enquêtes sur la page Détections.

Détections par catégorie d'attaque

Ce graphique fournit un moyen rapide de voir les types d'attaques susceptibles de menacer votre réseau et affiche le nombre de détections survenues dans chaque catégorie au cours de l'intervalle de temps sélectionné. Les actions relatives aux détections objectives sont répertoriées par type pour vous aider à hiérarchiser les détections les plus graves. Cliquez sur n'importe quel chiffre pour ouvrir une vue filtrée des détections correspondant à la valeur sélectionnée catégorie d'attaque.

Délinquants fréquents

Ce graphique montre les 20 appareils ou terminaux qui ont agi en tant que contrevenants lors d'une ou de plusieurs détections. Le système ExtraHop prend en compte le nombre de catégories d'attaques et de types de détection distincts, ainsi que les scores de risque des détections associés à chaque équipement afin de déterminer quels appareils sont considérés comme des récidivistes.

La taille de l' icône de rôle de l'équipement indique le nombre de types de détection distincts et la position de l'icône indique le nombre de catégories d'attaques distinctes. Cliquez sur l'icône d'un rôle pour afficher plus d'informations sur les catégories d'attaques et les types de détection associés à l'équipement. Cliquez sur le nom de l'équipement pour afficher propriétés de l'équipement.

En savoir plus sur la sécurité du réseau grâce au Tableau de bord Security Hardening.

Briefings sur les menaces

Les briefings sur les menaces fournissent des conseils actualisés dans le cloud concernant les événements de sécurité à l'échelle du secteur. En savoir plus sur les briefings sur les menaces.

Sélecteur de site et rapport exécutif

Vous pouvez spécifier les sites dont vous souhaitez consulter les données sur cette page. Les utilisateurs ayant accès au module NDR peuvent générer un rapport exécutif pour partager les résultats.

Sélecteur de site

Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Visualisez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour vous aider à trouver rapidement les données des équipements. Le sélecteur de site indique quand tous les sites ou certains sites sont hors ligne. Comme les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipements associés aux sites hors

ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site n'est disponible que depuis un console.

(module NDR uniquement) Rapport exécutif

Le rapport exécutif contient un résumé des principales détections et des principaux risques pour votre réseau. Cliquez **Générer un rapport** pour créer un fichier PDF à la demande contenant un résumé de la semaine dernière à partir des sites sélectionnés. Cliquez **Rapport sur le calendrier** pour créer un rapport exécutif planifié qui contient un résumé des détections pour un intervalle de temps spécifié et est envoyé par e-mail aux destinataires selon une fréquence configurée.