Vue d'ensemble du réseau

Publié: 2024-04-10

L'aperçu du réseau affiche une carte des détections sur votre réseau et une liste des délinquants par nombre de détections. La vue d'ensemble du réseau actualise la carte de détection et les données sur les délinquants toutes les minutes.

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

Basculer entre les catégories de détection

Vous pouvez basculer entre les vues qui affichent **Toutes les détections d'attaques** ou **Toutes les détections de performances**, en fonction des modules activés et de votre accès aux modules.

Délinquants lors de détections

Cette liste répertorie les délinquants, triés selon le nombre de détections où l'équipement ou le point de terminaison a agi comme un délinquant.

Voici quelques manières d'interagir avec la liste des délinquants :

- Cliquez sur un équipement ou un point de terminaison dans la liste pour mettre en évidence les détections associées sur la carte de détection, afficher les propriétés de l'équipement et accéder aux liens vers recherche de point de terminaison sites, détections, enregistrements ou paquets.
- En fonction de la catégorie de détection sélectionnée et du module de votre système, cliquez sur **Afficher toutes les détections d'attaques** ou **Afficher toutes les détections de performance** lien pour accéder au Détections page, filtré par catégorie de détection et regroupé par source.
- Sélectionnez le **Afficher les détections sans victimes** case à cocher pour afficher les détections qui n'incluent pas de victime participante. Par exemple, les scans SSL/TLS et certaines détections d'avertissement pour détecter des activités suspectes n'incluent qu'un délinquant.

Carte de détection

La carte de détection affiche le délinquant et la victime pour toutes les détections sélectionnées lors du basculement entre les catégories de détection.

Les cercles sont surlignés en rouge si l'équipement est apparu en tant que délinquant lors d' au moins une détection pendant l'intervalle de temps sélectionné et sont surlignés en bleu sarcelle si l' équipement est une victime.

Les participants sont connectés par des lignes étiquetées avec le type de détection ou le nombre de détections associés à la connexion, et les rôles des équipements sont représentés par une icône.

Voici quelques manières d'interagir avec la carte de détection :

- Cliquez sur un cercle pour afficher les propriétés de l'équipement et accéder aux liens vers recherche de point de terminaison sites, détections, enregistrements ou paquets.
- Cliquez sur une connexion pour afficher les détections associées.
- Passez la souris sur un cercle pour voir les étiquettes des équipements et surligner les connexions des appareils.

En savoir plus sur Détections.

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.