Tableau de bord Security Hardening

Publié: 2024-11-04

Le tableau de bord Security Hardening vous permet de surveiller les informations générales relatives aux menaces de sécurité potentielles sur votre réseau.

Chaque graphique du tableau de bord Security Hardening contient des visualisations des données de sécurité qui ont été générées via intervalle de temps sélectionné, organisé par région.

Vidéos Consultez la formation associée : Tableau de bord de sécurité

Note: À partir d'une console, vous pouvez afficher le tableau de bord Security Hardening pour chaque sonde réseau d'analyse de paquets. Cliquez sur la flèche vers le bas à côté du nom de la sonde dans la barre de navigation pour afficher le tableau de bord Security Hardening pour les autres capteurs.

Le tableau de bord Security Hardening est un tableau de bord intégré au système que vous ne pouvez pas modifier, supprimer ou ajouter à une collection partagée. Cependant, vous pouvez copier un graphique depuis le tableau de bord Security Hardening et ajoutez-le à tableau de bord personnalisé, ou vous pouvez faire une copie du tableau de bord et modifiez-le pour suivre les statistiques qui vous concernent.

Les informations suivantes résument chaque région et ses graphiques.

Renseignements sur les menaces

Observez le nombre de connexions et de transactions contenant des noms d'hôte, des adresses IP ou des URI suspects trouvés dans renseignement sur les menaces. Cliquez sur une valeur métrique bleue ou sur le nom d'une métrique dans la légende pour accéder à une métrique suspecte. Une page détaillée apparaît avec une icône de caméra rouge à côté de l'objet suspect. Cliquez sur l'icône rouge représentant une caméra pour en savoir plus sur la source de renseignements sur les menaces.

Note: Les métriques de renseignement sur les menaces affichent une valeur nulle pour l'une ou plusieurs des raisons suivantes :

- Votre abonnement ExtraHop RevealX ne contient pas de renseignements sur les menaces.
- Vous n'avez pas activé les renseignements sur les menaces pour votre système ExtraHop RevealX.
- Vous n'avez pas directement chargé de collections de menaces personnalisées sur votre capteurs. Contactez le support ExtraHop pour obtenir de l'aide lors du téléchargement d'une collecte des menaces personnalisée vers votre site géré par ExtraHop capteurs.
- Aucun objet suspect n'a été trouvé.

TLS - Séances

Observez le nombre de sessions TLS actives avec des suites de chiffrement faibles sur votre réseau. Vous pouvez voir quels clients et serveurs participent à ces sessions ainsi que les suites de chiffrement avec lesquelles ces sessions sont cryptées. Les suites de chiffrement DES, 3DES, MD5, RC4, nulles, anonymes et d'exportation sont considérées comme faibles car elles incluent un algorithme de chiffrement connu pour sa vulnérabilité. Les données chiffrées à l'aide d'une suite de chiffrement faible sont potentiellement dangereuses.

Vous pouvez également observer le nombre de sessions TLS établies avec TLS v1.0 et quels clients participent à ces sessions. Des vulnérabilités connues sont associées à TLS v1.0. Si vous disposez d'un nombre élevé de sessions TLS v1.0, pensez à configurer les serveurs pour qu'ils prennent en charge la dernière version de TLS.

TLS - Certificats

Observez les certificats TLS de votre réseau qui sont auto-signés, comportent un caractère générique, ont expiré ou expirent bientôt. Les certificats auto-signés sont signés par l'entité qui les

émet, plutôt que par une autorité de certification fiable. Bien que les certificats auto-signés soient moins chers que les certificats émis par une autorité de certification, ils sont également vulnérables aux attaques de type man-in-the-middle.

Un certificat générique s'applique à tous les sous-domaines de premier niveau d'un nom de domaine donné. Par exemple, le certificat générique *.company.com sécurise www.company.com, docs.company.com et customer.company.com. Bien que les certificats génériques soient moins chers que les certificats individuels, les certificats génériques présentent un risque accru s'ils sont compromis, car ils peuvent s'appliquer à un nombre illimité de domaines.

Scans de vulnérabilité

Observez quels appareils analysent les applications et les systèmes de votre réseau afin de détecter les points faibles et les cibles potentielles, tels que les appareils à valeur élevée. Dans le graphique de gauche, vous pouvez identifier les appareils qui envoient le plus de requêtes de numérisation, à savoir les requêtes HTTP associées à une activité d'analyse connue. Dans le graphique de droite, vous pouvez voir quels agents utilisateurs sont associés aux demandes d'analyse. L'agent utilisateur peut vous aider à déterminer si les demandes de scan sont associées à des scanners de vulnérabilités connus tels que Nessus et Qualys.

DNS

Observez les serveurs DNS les plus actifs sur votre réseau et le nombre total d'échecs de recherche DNS inversée rencontrés par ces serveurs. Un échec de recherche DNS inversée se produit lorsqu'un serveur émet une erreur en réponse à une demande d' enregistrement de pointeur (PTR) d'un client. Les échecs des recherches DNS inversées sont normaux, mais une augmentation soudaine ou régulière du nombre de défaillances sur un hôte spécifique peut indiquer qu'un attaquant analyse votre réseau.

Vous pouvez également observer le nombre de requêtes de mappage d'adresses et d'enregistrement de texte sur votre réseau. Une augmentation importante ou soudaine de ces types de requêtes peut indiquer la présence d'un tunnel DNS potentiel.