FAQ sur les simulations d'attaques

Publié: 2023-09-19

Voici quelques réponses aux questions fréquemment posées sur la détection des simulations d'attaques avec le système ExtraHop.

Qu'est-ce qu'un simulateur d'attaque ?

Un simulateur d'attaque est également connu sous le nom de simulation de brèche et d'attaque (BAS). Ces outils permettent aux analystes d'élaborer une campagne de menaces qui émule des techniques d'attaque afin d'évaluer la couverture des outils de sécurité.

Comment le système ExtraHop identifie-t-il les simulateurs d'attaque ?

Le système ExtraHop peut découvrir et classer automatiquement certains simulateurs d'attaque en fonction de l'activité du logiciel ou du protocole, puis attribuer un rôle de simulateur d'attaque à l'appareil. Vous pouvez également attribuer manuellement le rôle de simulateur d'attaque à n'importe quel dispositif.

En savoir plus sur les rôles des périphériques.

Comment le système ExtraHop détecte-t-il les simulations d'attaques ?

Le système ExtraHop applique des techniques d'apprentissage automatique et une surveillance basée sur des règles aux données des fils pour détecter les attaques réelles et simulées.

En savoir plus sur les détections.

À quoi puis-je m'attendre après avoir effectué une simulation d'attaque ?

Chaque détection possède une fiche de détection qui identifie la cause de la détection, la catégorie de détection, le moment où la détection s'est produite, le score de risque et les participants, tels que l'appareil qui exécute le simulateur d'attaque. Une carte de détection apparaît pour les techniques d'attaque simulées qui ont été générées par un simulateur d'attaque, tel que Mandiant Security Validation.

Les cartes de détection décrivent la manière dont le système ExtraHop détecte les techniques d'attaque et les comportements réels. Les simulateurs d'attaques simulent souvent le trafic d'attaque réel, mais des contraintes peuvent rendre le trafic simulé différent du trafic réel. En fonction de la simulation, une carte de détection peut ne pas décrire exactement comment la technique simulée a été détectée. Dans ce cas, le titre de la carte de détection comprendra [Simulation]. Par exemple, le nombre de tentatives de connexion infructueuses associées à une simulation d'attaque par force brute via le protocole Remote Desktop Protocol (RDP) peut être nettement inférieur au nombre de tentatives de connexion infructueuses lors d'une attaque par force brute dans le monde réel. Une détection **[Simulation] RDP Brute Force**apparaît, car cette simulation a été détectée avec une sensibilité accrue.