FAQ sur la simulation d'attaque

Publié: 2025-02-13

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'attaques ?

Un simulateur d'attaques est également connue sous le nom de simulation de brèche et d'attaque (BAS). Ces outils permettent aux analystes de créer une campagne contre les menaces qui imite les techniques d'attaque afin d'évaluer la couverture des outils de sécurité.

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

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

En savoir plus sur rôles de l'équipement.

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 filaires afin de détecter les attaques réelles et simulées.

En savoir plus sur détections.

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

Chaque détection possède un carte de détection qui identifie la cause de la détection, la catégorie de détection, le moment où la détection s'est produite, l'indice de risque et les participants, tels que l'équipement exécutant le simulateur d'attaques. Une carte de détection apparaît pour les techniques d'attaques simulées qui ont été générées par un simulateur d'attaque, telles que Mandiant Security Validation.

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