# Häufig gestellte Fragen zur Angriffssimulation

Veröffentlicht: 2025-02-12

Hier finden Sie Antworten auf häufig gestellte Fragen zur Erkennung von Angriffssimulationen mit dem ExtraHop-System.

### Was ist ein Angriffssimulator?

Ein Angriffssimulator wird auch als Breach- und Angriffssimulation (BAS) bezeichnet. Diese Tools ermöglichen es Analysten, eine Bedrohungskampagne zu erstellen, die Angriffstechniken emuliert, um die Reichweite der Sicherheitstools zu bewerten.

### Wie identifiziert das ExtraHop-System Angriffssimulatoren?

Das ExtraHop-System kann einige Angriffssimulatoren anhand von Software- oder Protokollaktivitäten automatisch erkennen und klassifizieren und dem Gerät dann eine Angriffssimulatorrolle zuweisen . Sie können die Geräterolle des Angriffssimulator auch manuell einem beliebigen Gerät zuweisen.

Erfahre mehr über Geräterollen.

### Wie erkennt das ExtraHop-System Angriffssimulationen?

Das ExtraHop-System wendet Techniken des maschinellen Lernens und regelbasierte Überwachung auf wire data an, um sowohl reale als auch simulierte Angriffe zu erkennen.

Erfahre mehr über Erkennungen.

### Was kann ich erwarten, nachdem ich eine Angriffssimulation ausgeführt habe?

Jede Erkennung hat eine Erkennungskarte das die Ursache der Entdeckung, die Erkennungskategorie, den Zeitpunkt der Erkennung, die Risikoscore und die Teilnehmer identifiziert, z. B. das Gerät, auf dem der Angriffssimulator ausgeführt wird. Für simulierte Angriffstechniken, die von einem Angriffssimulator wie Mandiant Security Validation generiert wurden, wird eine Erkennungskarte angezeigt.

Erkennungskarten beschreiben, wie das ExtraHop-System reale Angriffstechniken und -verhalten erkennt. Angriffssimulatoren simulieren häufig realen Angriffsverkehr, aber Einschränkungen können dazu führen, dass sich der simulierte Verkehr vom realen Verkehr unterscheidet. Je nach Simulation beschreibt eine Erkennungskarte möglicherweise nicht genau, wie die simulierte Technik erkannt wurde. In diesen Fällen enthält der Titel einer Erkennungskarte [Simulation]. Beispielsweise kann die Anzahl der fehlgeschlagenen Anmeldeversuche im Zusammenhang mit einem simulierten Brute-Force-Angriff über das Remote Desktop Protocol (RDP) erheblich niedriger sein als die Anzahl der fehlgeschlagenen Anmeldeversuche während eines echten Brute-Force-Angriff. EIN **[Simulation] RDP Brute Force** Die Erkennung erscheint, weil diese Simulation mit erhöhter Empfindlichkeit erkannt wurde.