Prioritäten der Analyse

Veröffentlicht: 2025-02-12

Das ExtraHop-System analysiert den Verkehr und sammelt Daten von allen erkannten Geräten auf einem einzigen Sensor. Jedes erkannte Gerät erhält eine Analyseebene, die bestimmt, welche Daten und Metriken für ein Gerät erfasst werden. Analyseprioritäten bestimmen, welche Analysestufe ein Gerät erhält.

Wichtig: Analyseprioritäten können sein zentral verwaltet von einer Konsole aus.

Video: Sehen Sie sich die entsprechende Schulung an: Analyse-Prioritäten

Analysestufen

Das ExtraHop-System analysiert Geräte intelligent und weist automatisch eine Analyseebene zu. Sie können die Analyseebene auch für Geräte und Gerätegruppen konfigurieren.

Hinweis: Datensätze und Pakete sind für alle Geräte auf ExtraHop-Systemen verfügbar, die mit einem Recordstore oder Packetstore konfiguriert sind, unabhängig von der Analyseebene.

Jedes Gerät erhält eine der folgenden Analysestufen.

Entdeckungsmodus

Das ExtraHop-System identifiziert bekannte Gerätehardware und -software, authentifizierte Benutzer sowie zugewiesene und zugehörige IP-Adressen. Das ExtraHop-System generiert auch Erkennungen und Diagramme, die die auf dem Gerät beobachtete Protokollaktivität zeigen. Alle Geräte erhalten mindestens diese Analysestufe, mit Ausnahme der L2-Elterngeräte.

Standardanalyse

Das ExtraHop-System enthält mindestens eine Woche lang L2-L3-Metrik- und Peer-Relationship-Daten, die Sie sofort anhand von Erkennungen, Diagrammen und Aktivitätskarten untersuchen können. Das ExtraHop-System identifiziert auch bekannte Gerätehardware und -software, authentifizierte Benutzer sowie zugewiesene und zugehörige IP-Adressen. Erfahren Sie, wie Gruppen für die Standardanalyse priorisieren.

Erweiterte Analyse

Das ExtraHop-System umfasst mindestens eine Woche lang L2-L7-Metriken aus über 50 Protokollen und Peer-Relationship-Daten, die Sie sofort anhand von Erkennungen, Diagrammen und Aktivitätskarten sowie benutzerdefinierten Dashboards, Berichten und Warnungen untersuchen können. Das ExtraHop-System identifiziert auch bekannte Gerätehardware und -software, authentifizierte Benutzer sowie zugewiesene und zugehörige IP-Adressen. Erfahren Sie, wie Gruppen für die erweiterte Analyse priorisieren oder ein einzelnes Gerät zu einer Beobachtungsliste hinzufügen.

L2-Elternanalyse

L2 Parent Analysis ist nur anwendbar, wenn L3 Discovery auf dem ExtraHop-System aktiviert ist. Mit Ausnahme von Gateways und Routern erhalten L2-Elterngeräte automatisch diese Analysestufe, die L2-L3-Protokollmetriken und Aktivitätskarten sammelt.

Strömungsanalyse

Ein Fluss Sensor sammelt Daten aus Flow-Logs anstelle von Paketen zur Analyse durch das ExtraHop-System. Geräte, die im Fluss erkannt wurden Sensoren automatisch diese Analysestufe erhalten. Systemeinstellungen für Analyseprioritäten sind für Fluss nicht verfügbar Sensoren, und Geräte in Flow Analysis können nicht zur Beobachtungsliste hinzugefügt werden.

Sehen Sie eine Tabelle, die vergleicht diese Analyseebenen.

Priorisierung von Geräten und Gruppen

Sie können die meisten Geräte zu einer Beobachtungsliste hinzufügen, um Erweiterte Analyse sicherzustellen, oder Sie können Gerätegruppen zu einer geordneten Liste hinzufügen, die Geräte für Advanced Analysis und Standard Analysis priorisiert.

Hier sind einige wichtige Überlegungen zur Priorisierung von Geräten auf der Beobachtungsliste:

- Geräte bleiben auf der Beobachtungsliste, auch wenn sie inaktiv sind, aber für inaktive Geräte werden keine Messwerte erfasst. Auch wenn sie inaktiv sind, bleiben Geräte auf der Beobachtungsliste Teil Ihrer Advanced Analysis-Kapazität.
- Die Anzahl der Geräte auf der Beobachtungsliste darf Ihre Erweiterte Analyse Analysis-Kapazität nicht überschreiten.
- Geräte können der Beobachtungsliste nur über eine Seite mit den Geräteeigenschaften oder der Gerätelistenseite hinzugefügt werden. Sie können der Beobachtungsliste von der Seite „Analyse-Prioritäten“ aus keine Geräte hinzufügen.
- Wenn du mehrere Geräte zur Beobachtungsliste hinzufügen möchtest, empfehlen wir dir eine Gerätegruppe erstellen und dann priorisieren Sie diese Gruppe für die erweiterte Analyse.
- Geräte, die L2 Parent Analysis oder Flow Analysis erhalten, können nicht zur Beobachtungsliste hinzugefügt werden.

Im Folgenden finden Sie einige wichtige Überlegungen zur Priorisierung von Gerätegruppen:

- Ordnen Gerät Gerätegruppen von der höchsten zur niedrigsten Priorität in der Liste an.
- Klicken und ziehen Sie Gruppen, um ihre Reihenfolge in der Liste zu ändern.

Standardmäßig füllt das ExtraHop-System die Stufen Advanced und Standard Analysis intelligent bis zur maximalen Kapazität aus. Im Folgenden finden Sie einige wichtige Überlegungen zu den Kapazitätsstufen und der automatischen Fülloption:

- Geräte, die in der Beobachtungsliste oder über eine priorisierte Gruppe priorisiert wurden, füllen zuerst die höheren Analyseebenen aus und dann von den Geräten, die am frühesten erkannt wurden.
- Geräte werden vom System automatisch für die erweiterte Analyse priorisiert, wenn das Gerät mit bestimmten Erkennungen verknüpft ist, wenn das Gerät eine externe Verbindung akzeptiert oder initiiert hat oder wenn auf dem Gerät gängige Angriffstools ausgeführt werden.
- Geräteeigenschaften wie Rolle, Hardware und Software, Protokollaktivität und Entdeckungshistorie können ebenfalls die Analysestufen bestimmen.
- Die Option Automatisch füllen ist standardmäßig aktiviert. Wenn diese Option deaktiviert ist, werden alle Geräte entfernt, die sich nicht in priorisierten Gruppen oder in der Beobachtungsliste befinden, und das ExtraHop-System legt die Priorität für jedes Gerät fest.
- Ihr ExtraHop-Abonnement und Ihre Lizenz bestimmen die maximale Kapazität.

Sehen Sie die Häufig gestellte Fragen zu Analyseprioritäten um mehr über die Kapazitäten und die Rangfolge auf Analyseebene zu erfahren.

Analysestufen vergleichen

Analyseebene	Funktionen	So erhalten Sie dieses Level
Entdeckungsmodus	• Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software	Geräte erhalten automatisch den Entdeckungsmodus, wenn sie sich nicht in Standard, Advanced oder L2 Parent Analysis befinden.

Analyseebene	Funktionen	So erhalten Sie dieses Level
	• Marke und Modell der Hardware	
Standardanalyse	• L2-L3-Metriken • Karten mit Aktivitäten • Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software • Marke und Modell der Hardware	Gerätegruppen für die Standardanalyse priorisieren.
Erweiterte Analyse	• L2-L7-Metriken • Benutzerdefinierte Metriken • Karten mit Aktivitäten • Erkennungen • Beobachtete Protokolle • IP-Adressen • Authentifizierte Benutzer • Software • Marke und Modell der Hardware	Gerätegruppen für Erweiterte Analyse priorisieren oder einzelne Geräte zur Beobachtungsliste hinzufügen.
L2-Elternanalyse (Gilt nur, wenn L3-Entdeckung ist aktiviert)	• L2-L3-Metriken • Karten mit Aktivitäten	L2-Elterngeräte erhalten automatisch L2 Parent Analysis, mit Ausnahme von Gateways und Routern.
Strömungsanalyse	• L2-L3-Metriken • Karten mit Aktivitäten • Beobachtete Protokolle • IP-Adresse • Eigenschaften der Cloud-Instanz • Eingeschränkte Erkennungsarten	Geräte erhalten automatisch eine Durchflussanalyse, wenn sie auf einem Flusssensor entdeckt werden.