Prioritäten der Analyse

Veröffentlicht: 2023-09-13

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

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

Analysestufen

Jedes Gerät erhält eine der folgenden Analysestufen.

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

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 beobachteten Protokollaktivitäten zeigen. Alle Geräte erhalten mindestens diese Analysestufe, mit Ausnahme der L2-Elterngeräte.

Standardanalyse

Das ExtraHop-System enthält mindestens eine Woche lang L2-L3-Metriken und Peer-Relationship-Daten, die Sie anhand von Erkennungen, Diagrammen und Aktivitätskarten sofort 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-Beziehungsdaten, die Sie sofort anhand von Erkennungen, Diagrammen und Aktivitätskarten sowie benutzerdefinierten Dashboards, Berichten und Benachrichtigungen untersuchen können. Das ExtraHop-System identifiziert auch bekannte Gerätehardware und -software, authentifizierte Benutzer sowie zugewiesene und zugehörige IP-Adressen. Erfahren Sie, wie Gruppen für 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 Analyseebene, die L2-L3-Protokollmetriken und Aktivitätskarten sammelt.

Strömungsanalyse

Ein Fluss Sensor sammelt Daten aus Flussprotokollen statt aus Paketen zur Analyse durch das ExtraHop-System. Geräte, die bei Fluss entdeckt wurden Sensoren erhalten automatisch diese Analyseebene. Die Systemeinstellungen für Analyseprioritäten sind für Fluss nicht verfügbar Sensoren, und Geräte in Flow Analysis können nicht zur Beobachtungsliste hinzugefügt werden.

Sehen Sie sich eine Tabelle an, die vergleicht diese Analyseebenen.

Geräte und Gruppen priorisieren

Das ExtraHop-System kann Hunderttausende von Geräten analysieren und automatisch bestimmen, welche Analysestufe jedes Gerät erhält. Sie können jedoch steuern, welche Geräte für Advanced und Standard Analysis priorisiert werden.

Die meisten Geräte können zu einer Beobachtungsliste hinzugefügt werden, um Erweiterte Analyse sicherzustellen, oder Sie können Gerätegruppen zu einer geordneten Liste hinzufügen, um sie für Advanced Analysis und Standard Analysis zu priorisieren.

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

- Geräte bleiben auf der Beobachtungsliste, auch wenn sie inaktiv sind, aber es werden keine Messwerte für inaktive Geräte erfasst.
- Die Anzahl der Geräte auf der Beobachtungsliste darf Ihre Erweiterte Analyse Analysis-Kapazität nicht überschreiten.
- Geräte können der Beobachtungsliste nur von einer Geräteeigenschaftenseite oder der Gerätelistenseite aus hinzugefügt werden. Sie können der Beobachtungsliste keine Geräte von der Seite Analyseprioritäten aus hinzufügen.
- Wenn Sie mehrere Geräte zur Beobachtungsliste hinzufügen möchten, empfehlen wir Ihnen eine Gerätegruppe erstellen und dann priorisieren Sie diese Gruppe für Advanced Analysis.
- Geräte, die L2 Parent Analysis oder Flow Analysis empfangen, können nicht zur Beobachtungsliste hinzugefügt werden.

Hier sind 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.
- Stellen Sie sicher, dass jedes Gerät in der Gruppe aktiv ist. Gruppen, die eine große Anzahl von Geräten enthalten, beanspruchen Kapazität und inaktive Geräte generieren keine Messwerte.
- Sie können nicht mehr als 200 Gerätegruppen für jede Ebene priorisieren.

Standardmäßig füllt das ExtraHop-System die Stufen Advanced und Standard Analysis automatisch bis zur maximalen Kapazität aus. Hier sind einige wichtige Überlegungen zu den Kapazitätsniveaus und der automatischen Fülloption:

- Geräte, die in der Beobachtungsliste oder über eine priorisierte Gruppe priorisiert wurden, füllen zuerst die höheren Analysestufen und dann die Geräte, die am frühesten entdeckt wurden.
- Geräte werden 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, Erkennungsverlauf und hoher Wert können ebenfalls die Analysestufen bestimmen.
- Die Option Automatisch ausfüllen 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 Kapazitäten auf Analyseebene zu erfahren.

Analysestufen vergleichen

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

Analyseebene	Funktionen	So erhalten Sie dieses Level
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.