Häufig gestellte Fragen zu Analyseprioritäten

Veröffentlicht: 2025-02-12

Hier finden Sie einige Antworten auf häufig gestellte Fragen zu Analyseprioritäten.

Wie funktionieren intelligente Analyseprioritäten?

Das ExtraHop-System priorisiert automatisch neue Geräte und kritische Infrastrukturgeräte wie Windows-Server für die erweiterte Analyse.

Wenn ein Gerät bereits vom System für Erweiterte Analyse priorisiert wurde, müssen Sie das Gerät nicht manuell zu einer priorisierten Gerätegruppe oder Beobachtungsliste hinzufügen. Wir empfehlen Ihnen, die vom System festgelegte Priorisierung zu berücksichtigen.

Benutzerkonfigurierte Prioritäten haben Vorrang vor den intelligenten Analyseprioritäten, die vom System angewendet werden.

Was ist die Rangfolge der Analyseprioritäten?

Die Beobachtungsliste, Gerätegruppen, die für Erweiterte Analyse konfiguriert sind, und dann die intelligenten ExtraHop-Regeln werden priorisiert, bis die Kapazität von Erweiterte Analyse voll ist.

Als Nächstes werden Gerätegruppen, die für die Standardanalyse konfiguriert sind, und dann die intelligenten ExtraHop-Regeln priorisiert, bis die Kapazität der Standardanalyse voll ist. Schließlich werden alle verbleibenden Geräte priorisiert.

Wie wird die Gerätekapazität für Analysestufen bestimmt?

Die Anzahl der Geräte, die höhere Analysestufen erhalten, hängt von Ihrem ExtraHop-Abonnement und Ihrer Lizenz ab.

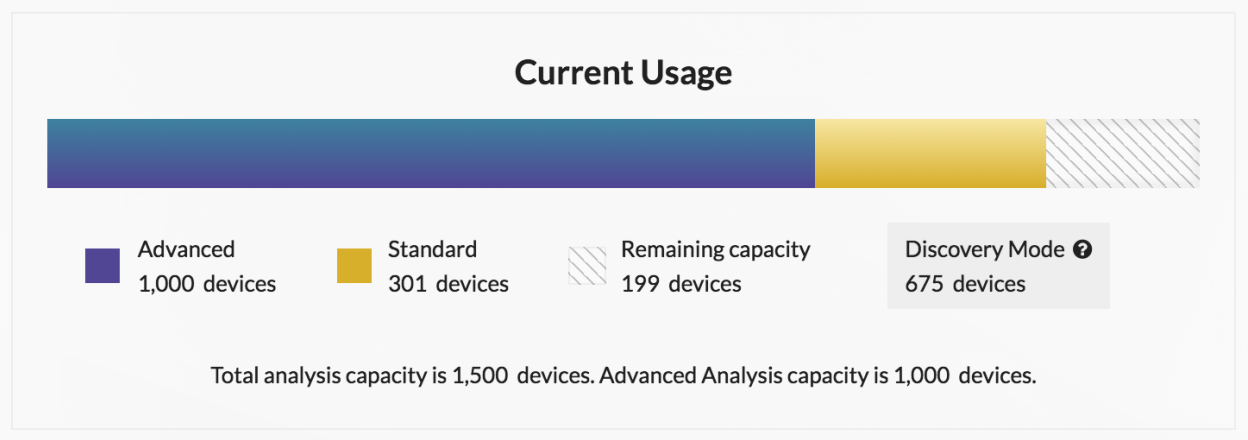
- Ihr Abonnement bestimmt die gesamte Analysekapazität, d. h. die Anzahl der Geräte, die Standard Analysis oder Erweiterte Analyse Analysis empfangen können.
- Ihre Lizenz bestimmt, wie viel von dieser Gesamtkapazität für Advanced Analysis, die höchste Analysestufe, verfügbar ist.

Beispielsweise beträgt die gesamte Analysekapazität für einen EDA 9200 50.000 gleichzeitig aktive Geräte. Bis zu 8.000 dieser aktiven Geräte können in die erweiterte Analyse aufgenommen werden. Weitere Informationen zur Analysekapazität für jedes ExtraHop-Abonnement erhalten Sie von Ihrem ExtraHop-Vertreter.

Wo finde ich meinen aktuellen Verbrauch?

Auf der Seite „ Analyseprioritäten“ wird ein Diagramm angezeigt, in dem auf einen Blick die Anzahl der Geräte , die auf jeder Ebene analysiert werden, im Vergleich zur verbleibenden Analysekapazität bewertet wird. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Analyse-Prioritäten**.

Die lizenzierten Gesamtkapazitäten werden unter dem Balkendiagramm angezeigt.



Woher weiß ich, welche Geräte auf der Beobachtungsliste stehen?

Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`, klicken Sie auf Systemeinstellungen Symbol und dann klicken **Analyse-Prioritäten**. Klicken Sie oben auf der Seite auf **Sehen Sie sich die Beobachtungsliste an**.

Wie füge ich mehrere Geräte zur Beobachtungsliste?

Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`. Klicken Sie oben auf der Seite auf **Vermögenswerte** und klicken Sie dann **Geräte** im linken Bereich. Suchen Sie auf der Gerätelistenseite nach Geräten und klicken Sie dann auf das Kontrollkästchen neben jedem Gerät, das Sie zur Beobachtungsliste hinzufügen möchten. Klicken Sie dann auf **Zur Watchlist hinzufügen** in der oberen rechten Ecke der Seite.

Weitere Informationen finden Sie unter Gerät zur Beobachtungsliste hinzufügen.

Welches Analyselevel erhalten benutzerdefinierte Geräte?

Maßgeschneiderte Geräte kann jede Analysestufe erhalten. Du kannst eine Gerätegruppe erstellen mit all Ihren benutzerdefinierten Geräten und priorisieren Sie diese Gruppe für die erweiterte oder die Standardanalyse. Oder du kannst füge ein individuelles Gerät zur Beobachtungsliste.

Welche Analysestufe unterstützt benutzerdefinierte Metriken?

Benutzerdefinierte Metriken sind nur in Erweiterte Analyse verfügbar. Wenn Sie benutzerdefinierte Messwerte für ein bestimmtes Gerät sehen möchten, priorisieren Sie eine Gruppe, die das Gerät enthält, oder fügen Sie das Gerät zur Beobachtungsliste hinzu.

Welche Analyseebene unterstützt Trigger?

EIN Auslöser wird für jedes Gerät ausgeführt, dem es zugewiesen ist, unabhängig von der Analyseebene. Die Analyseebene eines Gerät hat keinen Einfluss darauf , wann der Auslöser ausgeführt wird. Wenn jedoch ein einem Gerät zugewiesener Auslöser benutzerdefinierte Messwerte erfasst, müssen Sie das Gerät für die erweiterte Analyse priorisieren, bevor Sie die benutzerdefinierten Metrikdaten anzeigen können.

Wie ermittle ich die Analysestufe für ein Gerät?

Finde ein Gerät und klicken Sie dann auf den Gerätenamen, um das zu öffnen Seite „Geräteübersicht“. Die Analyseebene wird im Abschnitt mit den Geräteeigenschaften angezeigt.

Klicken Sie in einer Geräteliste auf die Spalte Analyseebene, um Geräte nach Ebene zu sortieren.

Extrahieren Sie die Geräteliste über die REST-API und fügen Sie eine Option hinzu, um nach Analyseebene zu filtern. Vollständige Schreibrechte sind erforderlich, um Befehle über die REST-API auszuführen.

Empfangen meine Geräte immer noch Softwarebeobachtungen, wenn sie sich in der Standardanalyse befinden?

Ja, Softwarebeobachtungen können für Geräte der Stufen Discovery, Standard oder Erweiterte Analyse erstellt werden. Softwarebeobachtungen helfen dem System dabei, kritische Geräte automatisch zu priorisieren. Geräte, die 30 Tage lang inaktiv sind, verlieren jedoch ihre auf Softwarebeobachtung basierende Priorisierung.

Was passiert, wenn ein priorisiertes Gerät inaktiv wird?

Ein Gerät kann im Laufe der Zeit inaktiv werden, wenn das Gerät in den letzten 30 Minuten keine Daten gesendet oder empfangen hat.

Wenn ein Gerät für ein bestimmtes Protokoll inaktiv ist und dieses Gerät zu einer priorisierten Gerätegruppe gehört, kann das Gerät bis zu 96 Stunden lang in der Erweiterten Analyse oder Standardanalyse verbleiben. Beispielsweise wird eine TLS-Server-Gerätegruppe für Erweiterte Analyse priorisiert. Ein Server, der normalerweise TLS-Anfragen empfängt, ist in dieser Gruppe enthalten. Wenn der Server in den letzten 30 Minuten keine TLS-Daten gesendet oder empfangen hat, aber weiterhin Daten über andere Protokolle sendet und empfängt, verbleibt der Server als Teil der TLS-Server-Gerätegruppe in Erweiterte Analyse. Wenn der Server nach 96 Stunden immer noch über das TLS-Protokoll inaktiv ist, ist der Server kein Mitglied der TLS-Servergruppe mehr und empfängt möglicherweise keine erweiterte Analyse mehr.

Geräte auf der Beobachtungsliste befinden sich immer in Erweiterte Analyse. Ein inaktives Gerät, das auf der Beobachtungsliste steht, verbraucht weiterhin Speicherplatz in Ihrer Erweiterte Analyse Analysekapazität, auch wenn das Gerät inaktiv ist.

Geräte, die Teil einer Gerätegruppe sind, verbrauchen Ihre Advanced Analysis- oder Standard Analysis-Kapazität nicht, nachdem sie inaktiv geworden sind. Wenn das Gerät wieder aktiv wird, erhält es Erweiterte Analyse oder Standard Analysis, basierend auf der konfigurierten Priorität für dieses Gerät.