Häufig gestellte Fragen zu Erkennungen

Veröffentlicht: 2024-04-10

Hier finden Sie Antworten auf häufig gestellte Fragen zu Erkennungen.

Wie unterscheiden sich Erkennungen von Warnungen?

Warnmeldungen und Erkennungen sind insofern ähnlich, als sie beide Informationen über die Bedingungen in Ihrem Netzwerk liefern. In der folgenden Tabelle wird beschrieben, wie sie sich unterscheiden. Warnmeldungen bieten Konfigurierte Warnbedingungen bestimmen, wann eine Alarm generiert wird.

	Warnmeldungen	Erkennungen
Wie werden sie generiert?	Nach Bedingungen, die Sie in den Alert-Einstellungen definieren. Sie können Trend- oder Schwellenwertwarnungen konfigurieren.	Automatisch anhand Ihrer Netzwerkdaten vom ExtraHop Machine Learning Service beobachtet.
Wie sehe ich sie an?	Klicken Sie **Warnmeldungen** aus dem Hauptmenü des ExtraHop-Systems.	Klicken Sie **Erkennungen** aus dem Hauptmenü des ExtraHop-Systems.
Wie richte ich E-Mail-Benachrichtigungen ein?	Du kannst Hinzufügen einer Benachrichtigung zu einer Alert-Konfiguration um E-Mails zu senden, wenn die Alarmbedingungen erfüllt sind.	Du kannst eine Benachrichtigungsregel erstellen um E-Mails über Entdeckungen zu versenden, die bestimmten Kriterien entsprechen.
Was sind die Vorteile?	Sie entscheiden, welche Geräte und Dienste mit hoher Priorität überwacht werden sollen, und bestimmen den Grad der Änderungen, die zu Benachrichtigungen führen.	Bemerkenswerte Änderungen an Ihrem Netzwerkverhalten werden automatisch angezeigt. Indem Sie Feedback zu Erkennungen geben, helfen Sie dem Machine Learning Service-Algorithmus, Ihr Netzwerk besser zu verstehen.

Was ist ein Risikoscore? (Nur ExtraHop Reveal (x))

EIN Risikoscore gibt den Schweregrad einer Erkennung an und wird auf der Grundlage der Wahrscheinlichkeit eines Angriffs, der Schwierigkeit, die Erkennung auszunutzen, und des Ausmaßes der Auswirkungen auf Ihren Betrieb berechnet.

Die Risikowerte sind in einen der folgenden farbcodierten Schweregrad gruppiert:

- Rot = 80-99
- Oranje = 31-79
- Gelb = 1-30

Für eine einzelne Erkennung wird keine Risikoscore angezeigt, wenn für diese Erkennung keine Bewertung und Definition einer Bewertung vorgenommen wurde.

Warum kann ich keine Quellgerätedetails für eine Erkennung anzeigen?

Wenn die Quelle einer Erkennung ein Gerät ist, das vom ExtraHop-System nicht erkannt wurde, zeigt die Erkennung nur die IP-Adresse und den Hostnamen des Gerät an, falls verfügbar. Sie können den Mauszeiger über das unentdeckte Gerät bewegen, um die Geolokalisierung der IP-Adresse und einen Link zur ARIN Whois-Website zu sehen.

Wie weit liegen die Funde zurück?

Erkennungen durch maschinelles Lernen werden eine Woche nach dem Verbindungsaufbau mit dem Dienst identifiziert. Der Dienst identifiziert dann in Zukunft alle neuen Erkennungen.

Beachten Sie, dass der Machine Learning Service vier Wochen (28 Tage) an Daten benötigt, um einen erwarteten Bereich von Metrikwerten zu berechnen. Der erwartete Bereich entspricht dem normalen Netzwerkverhalten. Die Datenverarbeitung ist in der Regel innerhalb weniger Stunden abgeschlossen.

Kann ich über einen Proxy eine Verbindung zum Machine Learning Service herstellen?

Der Machine Learning Service unterstützt implizite und explizite Proxys. Der Proxy erfordert , dass DNS alle *.extrahop.com-Domains auflöst, und der ausgehende 443-Port ist für alle IP-Adressen im Internet geöffnet. Diese Einstellungen werden in der Firewall für die Quell-IP-Adresse des Proxys implementiert.

Weitere Informationen zur Konfiguration eines expliziten Proxys finden Sie unter Stellen Sie über einen Proxy eine Verbindung zu ExtraHop Cloud Services her.

Welche Daten werden vom ExtraHop-System an den Machine Learning Service gesendet?

Der Machine Learning Service nutzt die einzigartigen Verarbeitungsfunktionen des ExtraHop-Systems, um wire data für Hunderte von Metriken vor Ort „vorzuverarbeiten“. Das ExtraHop-System verschlüsselt Metrikwerte und IP-Adressen, die an den Machine Learning Service gesendet werden. Das ExtraHop-System sendet keine benutzerdefinierten Metriken oder vertraulichen Daten wie Dateinamen, Zeichenketten oder Nutzdaten.

Wie sicher sind Erkennungen?

Erkennungen sind so konzipiert, dass sie von Anfang bis Ende sicher sind. Im Gegensatz zu einer typischen SaaS-Lösung erfassen Erkennungen keine Nutzlasten, Dateinamen, Zeichenfolgen oder andere Datenkategorien, die vertrauliche Informationen enthalten könnten. Der ExtraHop Machine Learning Service hat die SOC 2, Type 1-Konformitätszertifizierung erhalten.

Wie füge ich meinem ExtraHop-System eine neue oder aktualisierte Lizenz für den Machine Learning Service hinzu?

Wenn Sie ein neues ExtraHop-System gekauft haben, das eine Lizenz für den Machine Learning Service beinhaltet, erhalten Sie eine E-Mail mit einem neuen Produktschlüssel. Folgen Sie den Anweisungen zu registrieren Sie Ihr Gerät.

Wenn Sie eine Lizenz für den Machine Learning Service hinzugefügt haben, wird Ihre aktualisierte Lizenz automatisch zu Ihrem ExtraHop-System hinzugefügt, muss aber trotzdem angewendet werden. Folgen Sie den Anweisungen zu eine aktualisierte Lizenz anwenden.

Warum erhalte ich bestimmte Erkennungen durch maschinelles Lernen nicht?

Der Machine Learning Service unterstützt Versionen der ExtraHop-Firmware für ungefähr 15 Monate nach der Veröffentlichung der Firmware. Wenn Sie Ihre ExtraHop-Firmware länger als 15 Monate nicht aktualisieren, erhalten Sie möglicherweise nicht die neuesten aktualisierten und neuen Erkennungen vom Machine Learning Service. Kontaktieren Sie den ExtraHop Support für Unterstützung bei einem Firmware-Upgrade von Einen Fall im Kundenportal erstellen (erfordert Anmeldung).

Kann ich nach Ablauf meiner Machine Learning Service-Lizenz meine früheren Erkennungen immer noch einsehen?

Ja, frühere Erkennungen bleiben in Ihrem ExtraHop-System verfügbar.