Bedrohungssammlungen verwalten

Veröffentlicht: 2024-07-02

ExtraHop RevealX kann sich bewerben Bedrohungsinformationen zu Ihrer Netzwerkaktivität auf der Grundlage von Bedrohungssammlungen, die von Extrahop, CrowdStrike oder anderen kostenlosen und kommerziellen Quellen bereitgestellt werden.

Bevor Sie beginnen

- Erfahre mehr über Bedrohungsinformationen.
- Das musst du haben System- und Zugriffsadministrationsrechte auf jeder Konsole und jedem Sensor zur Verwaltung von Bedrohungssammlungen.
- Wenn Ihre ExtraHop-Bereitstellung eine Konsole umfasst, empfehlen wir Ihnen Transfermanagement Verbinden Sie alle angeschlossenen Sensoren mit der Konsole, um die integrierten Bedrohungssammlungen in Ihrem gesamten System zu aktivieren oder zu deaktivieren.

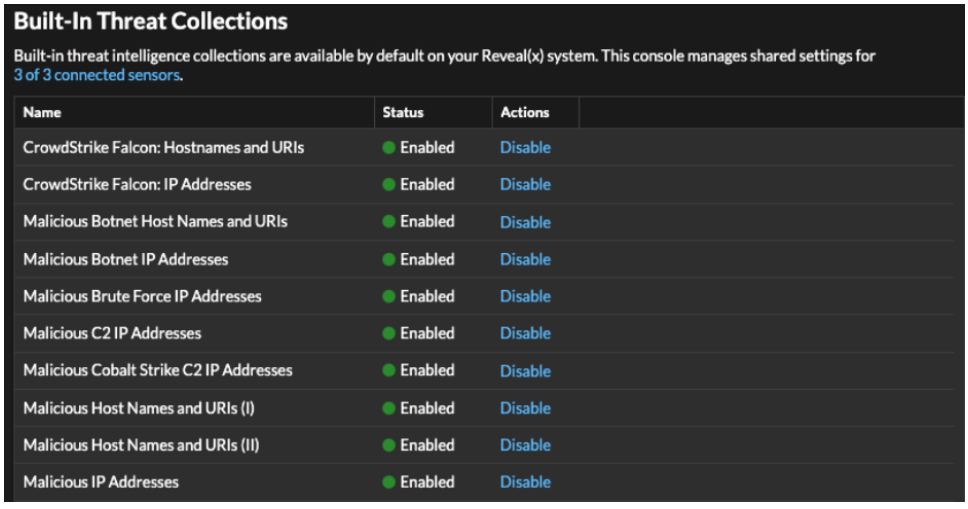
Integrierte Bedrohungssammlungen aktivieren oder deaktivieren

Integrierte Bedrohungssammlungen von ExtraHop und CrowdStrike identifizieren Anzeichen für eine Gefährdung im gesamten System.

Aktivierte Bedrohungssammlungen aktualisieren automatisch Systeme , die mit ExtraHop Cloud Services verbunden sind. Sie können die Konnektivität auf der ExtraHop Cloud-Dienste Seite in den Administrationseinstellungen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie in der Tabelle Integrierte Bedrohungssammlungen auf **Aktiviere** oder **Deaktiviert** in der Spalte Aktionen.

   Das System sucht automatisch alle 6 Stunden nach Updates für ExtraHop- und CrowdStrike-Bedrohungssammlungen.



Laden Sie eine Bedrohungssammlung hoch

Laden Sie Bedrohungssammlungen aus kostenlosen und kommerziellen Quellen hoch, um im gesamten ExtraHop-System Anzeichen für eine Gefährdung zu identifizieren. Da Bedrohungsdaten häufig (manchmal täglich) aktualisiert werden, müssen Sie möglicherweise eine Bedrohungssammlung mit den neuesten Daten aktualisieren. Wenn Sie eine Bedrohungssammlung mit neuen Daten aktualisieren, wird die Sammlung gelöscht und ersetzt und nicht an eine bestehende Sammlung angehängt.

Sie müssen Bedrohungssammlungen einzeln auf Ihre Konsole und auf alle angeschlossenen Sensoren hochladen.

Im Folgenden finden Sie einige Überlegungen zum Hochladen von Bedrohungssammlungen.

- Benutzerdefinierte Bedrohungssammlungen müssen in Structured Threat Information eXpression (STIX) als komprimierte TAR-Dateien wie .TGZ oder TAR.GZ formatiert werden. RevealX unterstützt derzeit Uploads der STIX-Dateiversionen 1.0 - 1.2.
- Sie können Bedrohungssammlungen direkt auf RevealX 360 hochladen, um sie selbst zu verwalten Sensoren. Wenden Sie sich an den ExtraHop-Support, um eine Bedrohungssammlung auf ExtraHop-Managed hochzuladen Sensoren.
- Die maximale Anzahl an Observables, die eine Bedrohungssammlung enthalten kann, hängt von Ihrem Sensorspeicher und Ihrer Lizenz ab. Um sicherzustellen, dass Uploads innerhalb der Grenzen Ihrer Sensoren und Ihrer Lizenz erfolgreich sind, empfehlen wir, Sammlungen in Dateien mit weniger als 3.000 Observables mit einer Gesamtgröße von weniger als 1 Million Observables aufzuteilen. Weitere Informationen zu Lizenz- und Plattformbeschränkungen für das Hochladen von Bedrohungssammlungen erhalten Sie von Ihrem ExtraHop-Vertreter.
- Du kannst Laden Sie STIX-Dateien über die REST-API hoch.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie **Benutzerdefinierte Sammlungen verwalten**.
4. Klicken Sie **Neue Kollektion hochladen**.
5. Geben Sie im Feld Sammlungs-ID eine eindeutige Sammlungs-ID ein. Die ID darf nur alphanumerische Zeichen enthalten und Leerzeichen sind nicht zulässig.
6. Klicken Sie **Wählen Sie eine Datei** und wähle eine `.tgz` Datei, die eine STIX enthält.
7. Geben Sie einen Anzeigenamen in das Feld Anzeigename ein.
8. Klicken Sie **Sammlung hochladen**.
9. Wiederhole diese Schritte für alle Konsolen und jeder ist verbunden Sensor.

Einen TAXII-Feed hinzufügen

Bedrohungssammlungen können über das TAXII-Protokoll (Trusted Automated Exchange of Intelligence Information) in Ihre Umgebung übertragen werden.

TAXII-Feeds können in ihrer Qualität oder Relevanz für Ihre Umgebung variieren. Um die Genauigkeit zu gewährleisten und das Rauschen zu reduzieren, empfehlen wir, nur Feeds aus zuverlässigen Quellen hinzuzufügen, die qualitativ hochwertige Bedrohungsdaten liefern.

Bevor Sie beginnen

- TAXII-Feed-Indikatoren werden von ExtraHop Cloud Services verarbeitet. Das ExtraHop-System muss verbunden mit ExtraHop Cloud Services um einen TAXII-Feed hinzuzufügen.
- TAXII-Feeds können nur von Benutzern mit NDR-Modulzugriff und Verwaltung von einer Konsole aus verwaltet werden Privilegien.

- TAXII-Feed-Indikatoren werden nur an angeschlossene Sensoren geliefert, auf denen die Firmware-Versionen 9.6.0 und höher ausgeführt werden.
- RevealX unterstützt derzeit TAXII-Feeds für die TAXII-Versionen 2.0 - 2.1, die die STIX-Dateiversionen 2.0 - 2.1 enthalten

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Bedrohungsinformationen**.
3. Klicken Sie im TAXII-Feed-Bereich auf **TAXII Feed hinzufügen**.
4. Geben Sie im Feld Name einen eindeutigen Namen für den TAXII-Feed ein.
5. Geben Sie im Feld TAXII Server Discovery URL die Discovery-URL für Ihren TAXII-Feed-Anbieter ein.
6. Wählen Sie im Drop-down-Menü TAXII-Version die TAXII-Protokollversion des Feeds aus.
7. Wählen Sie einen Authentifizierungstyp aus.
   - Keine Authentifizierung
   - Grundlegende Authentifizierung

     Geben Sie den Benutzernamen und das Passwort für den Ziel-Feed ein.
8. Geben Sie ein Zertifikat für den Zielfeed an.
   - Kein Zertifikat
   - Basiszertifikat

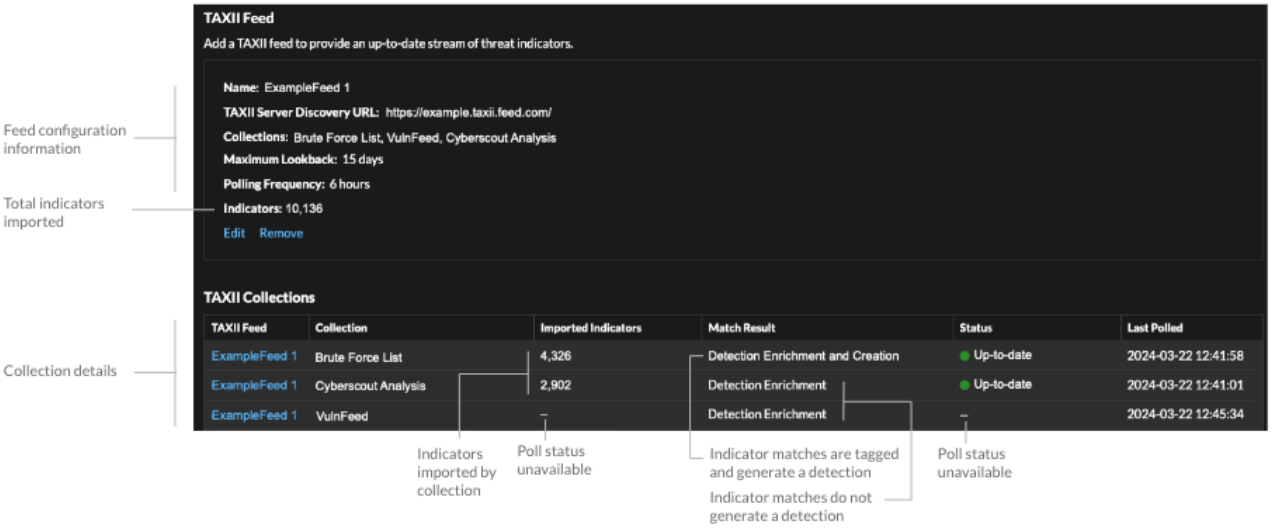
     Kopieren Sie den Inhalt der PEM-kodierten Zertifikatskette und fügen Sie ihn in das Feld für das Basiszertifikat ein. Es muss ein gültiger Vertrauenspfad vom Zertifikat zu einem vertrauenswürdigen Stammverzeichnis existieren.
9. Klicken Sie **Verbindung testen** um URL -, Authentifizierung- und Zertifikatseinstellungen zu bestätigen.
10. Klicken Sie **Weiter**.
11. Wählen Sie aus dem Drop-down-Menü Sammlungen zur Anreicherung die Bedrohungssammlungen aus , die zu einem verdächtigen Tag führen, wenn ein Indikator übereinstimmt.
12. Wählen Sie aus dem Drop-down-Menü Sammlungen für Erkennungserstellung die Bedrohungssammlungen aus, die zu einer Erkennung führen, wenn ein Indikator zutrifft .

    Hinweis Sie können eine Sammlung sowohl der Anreicherung als auch der Erkennungserstellung zuweisen. Wenn eine Sammlung nicht der Anreicherungsoption zugewiesen ist, wird die Sammlung während der Umfrage nicht aktualisiert und Indikatoren aus der Sammlung werden nicht in Ihrem System angezeigt.
13. Geben Sie im Feld Maximaler Lookback die Anzahl der Tage in der Vergangenheit ein, an denen Sie Indikatoren aus der Bedrohungssammlung akzeptieren möchten.

    Sie können diesen Wert auf eine Zahl zwischen 1 und 15 Tagen festlegen. Der Feed akzeptiert nur Indikatoren, die während dieser Lookback-Periode erstellt wurden.
14. Geben Sie im Feld Abfragehäufigkeit die Anzahl der Stunden zwischen der Abfrage des TAXII-Feeds nach Updates zur Bedrohungssammlung ein.

    Sie können diesen Wert auf eine Zahl zwischen 1 und 24 Stunden festlegen.
15. Klicken Sie **Speichern**.

Informationen zur TAXII-Feed-Konfiguration werden im Abschnitt TAXII-Feed der Threat Intelligence-Seite angezeigt, einschließlich des angegebenen Lookback-Zeitraums, der Abfragehäufigkeit und der Gesamtzahl der im Feed enthaltenen Indikatoren. Die Tabelle TAXII Collections enthält Details zu den einzelnen Sammlungen im Feed.



Hier sind einige Überlegungen zu TAXII-Feeds:

- Die Zeit, die für die Abfrage der TAXII-Feed- und Prozessindikatoren benötigt wird, basiert auf der Anzahl der Indikatoren im Feed. Als Referenz: Die Abfrage eines Feeds mit 500.000 Indikatoren im angegebenen Lookback-Zeitraum kann eine Stunde oder länger dauern.
- Indikatortypen, die vom ExtraHop-System nicht erkannt werden, gutartige Endpunktindikatoren und als gesperrt markierte Indikatoren werden bei der Umfrage aus dem Feed entfernt.
- In der TAXII-Sammeltabelle wird der Abholstatus mit einem Bindestrich (-) angezeigt, bis die Abholung auf dem neuesten Stand ist. Wenn dieser Status nicht auf aktuell gesetzt wird, testen Sie Ihre Verbindung zum TAXII-Server und überprüfen Sie dann Ihren TAXII-Feed-Anbieter, um sicherzustellen, dass die Sammlung noch im Feed vorhanden ist, dass Ihre Anmeldedaten Zugriff auf die Sammlung gewähren und dass Sie die vom Anbieter festgelegten Abfragelimits nicht überschritten haben. Ein teilweiser Aktualisierungsstatus wird angezeigt, wenn eine Sammlung während der Abfrage nicht vollständig aktualisiert wird. Teilaktualisierungen können erfolgen, wenn die Abfrage unerwartet unterbrochen wurde oder wenn ein Ratenlimit des Anbieters erreicht wurde.