Bedrohungssammlungen verwalten

Veröffentlicht: 2023-09-14

ExtraHop Reveal (x) kann sich bewerben Bedrohungsinformationen zu Ihren Netzwerkaktivitäten auf der Grundlage von Bedrohungssammlungen, die von Extrahop, Partnerintegrationen oder anderen kostenlosen und kommerziellen Quellen bereitgestellt werden.

Informationen zum Hinzufügen von Bedrohungsinformationen von CrowdStrike finden Sie unter Integrieren Sie Reveal (x) 360 mit CrowdStrike.

Bevor Sie beginnen

- Erfahre mehr über Bedrohungsinformationen.
- Du musst haben Rechte für die System- und Zugriffsadministration auf jeder Konsole und jedem Sensor, um Bedrohungssammlungen zu verwalten.

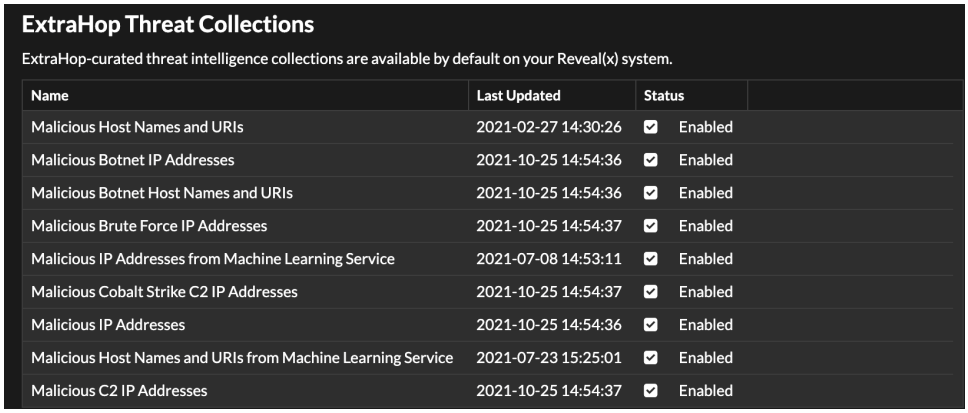
Von ExtraHop kuratierte Bedrohungssammlungen aktivieren oder deaktivieren

Die Bedrohungssammlungen von ExtraHop identifizieren Hinweise auf Sicherheitslücken im gesamten System.

Bedrohungssammlungen von ExtraHop aktualisieren automatisch Systeme, die mit den ExtraHop Cloud Services verbunden sind. Sie können die Konnektivität auf dem 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 dann klicken **Bedrohungsinformationen**.
3. Wählen oder deaktivieren Sie in der ExtraHop Threat Intelligence-Tabelle die **Aktiviert** Checkbox in der Spalte Status.

   Das System sucht automatisch alle 12 Stunden nach Aktualisierungen der von ExtraHOP kuratierten Bedrohungssammlungen. Die Spalte Letzte Aktualisierung gibt das Datum und die Uhrzeit der letzten Aktualisierung an.



Laden Sie eine Bedrohungssammlung hoch

Laden Sie Bedrohungssammlungen aus kostenlosen und kommerziellen Quellen hoch, um Hinweise auf eine Gefährdung im gesamten ExtraHop-System 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 TAR.GZ -Dateien formatiert werden. Reveal (x) unterstützt derzeit STIX Version 1.0 — 1.2.
- Sie können Bedrohungssammlungen zur Selbstverwaltung direkt auf Reveal (x) 360 hochladen Sensoren. Wenden Sie sich an den ExtraHop-Support, um eine Bedrohungssammlung auf ExtraHop-Managed hochzuladen Sensoren.
- Die maximale Anzahl von Observables, die eine Bedrohungssammlung enthalten kann, hängt von Ihrer Plattform und Lizenz ab. Weitere Informationen 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 dann klicken **Bedrohungsinformationen**.
3. klicken **Benutzerdefinierte Sammlungen verwalten**.
4. klicken **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 **Datei wählen** und wähle eine `.tgz` Datei, die eine STIX enthält.
7. Geben Sie einen Anzeigenamen in das Feld Anzeigename ein.
8. klicken **Sammlung hochladen**.
9. Wiederholen Sie diese Schritte für jedes verbundene Sensor und auf allen Konsolen.