Bedrohungssammlungen verwalten

Veröffentlicht: 2024-01-22

ExtraHop Reveal (x) 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.

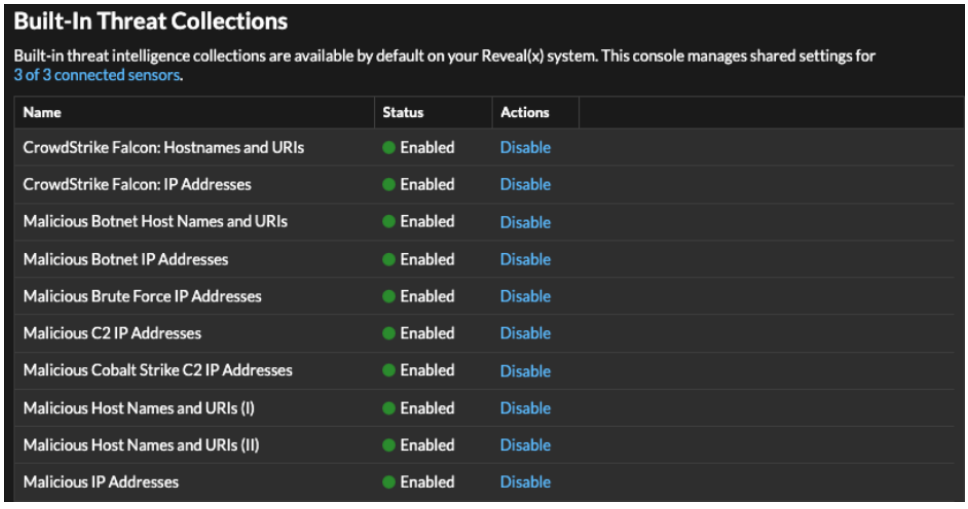
Integrierte Bedrohungssammlungen aktivieren oder deaktivieren

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 überprüfen 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. Reveal (x) unterstützt derzeit die STIX-Versionen 1.0 - 1.2.
- Sie können Bedrohungssammlungen direkt auf Reveal (x) 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. Wiederholen Sie diese Schritte für jede Verbindung Sensor und auf allen Konsolen.