

Integrieren Sie Reveal (x) 360 mit CrowdStrike

Veröffentlicht: 2024-01-22

Integrieren Sie ExtraHop Reveal (x) 360 mit CrowdStrike, um mehr Sichtbarkeit und Kontrolle über Ihre Geräte zu gewährleisten.

Systemanforderungen

ExtraHop Enthüllen (x) 360

- Ihr Benutzerkonto muss über Berechtigungen für Reveal (x) 360 für die System- und Zugriffsverwaltung oder das Cloud-Setup verfügen.
- Ihr Reveal (x) 360-System muss mit einem ExtraHop verbunden sein Sensor mit Firmware-Version 8.8 oder höher. Version 8.9 oder höher ist erforderlich, um die Integrationsoption für die Geräteeindämmung zu aktivieren.
- Ihr Reveal (x) 360-System muss [verbunden mit ExtraHop Cloud Services](#).

CrowdStrike

- Sie müssen das von ExtraHop bereitgestellte Sicherheitstoken in Ihrer Willkommens-E-Mail oder Ihrer CrowdStrike-API-Client-ID, Ihrem Client-Geheimnis und Ihrem Endpunkt haben.



Hinweis Wenn Sie Ihr ExtraHop-System aktualisieren, müssen Sie neue Anmeldedaten eingeben, um neue Integrationsoptionen zu konfigurieren.

- Der Umfang des CrowdStrike-API-Clients muss READ-Berechtigungen für Indikatoren (Falcon) enthalten, um Integrationsoptionen für die Anzeige von Links zu CrowdStrike-Geräten oder CrowdStrike Falcon-Bedrohungsinformationen zu ermöglichen.
- Der Umfang des CrowdStrike-API-Clients muss die LESE- und WRITE-Berechtigungen für Hosts enthalten, um die Integrationsoption zur Geräteeindämmung zu aktivieren.

Konfigurieren Sie die CrowdStrike-Integration

1. Melden Sie sich beim Reveal (x) 360-System an.
2. Klicken Sie auf das Symbol Systemeinstellungen  und klicken Sie dann **Integrationen**.
3. Klicken Sie auf die CrowdStrike-Kachel.
4. Wählen Sie eine der folgenden Optionen:
 - klicken **Sicherheitstoken eingeben** wenn Sie ein Token von ExtraHop erhalten haben, als Sie sich für eine kostenlose Testversion angemeldet haben.
 1. Fügen Sie das Sicherheitstoken aus Ihrer Willkommens-E-Mail in das **CrowdStrike-Sicherheitstoken** Feld.
 2. klicken **Verbinde**.
 - klicken **Geben Sie die Client-ID und das Geheimnis ein**.
 1. Geben Sie Ihre CrowdStrike-Client-ID in das Feld API-Client-ID ein.
 2. Geben Sie Ihr CrowdStrike-Client-Geheimnis in das Feld API-Client-Secret ein.
 3. Wählen Sie Ihren CrowdStrike-API-Regionen-Endpunkt aus der Dropdownliste aus.
 4. klicken **Verbindung testen** um sicherzustellen, dass das ExtraHop-System mit CrowdStrike Falcon kommunizieren kann.
 5. klicken **Verbinde**.
5. Optional: Konfigurieren Sie eine der folgenden Integrationsoptionen:

 **Hinweis** Die Integration kann nicht mehr als 50.000 Gesamtindikatoren aus CrowdStrike importieren.

- Wählen **Links zu CrowdStrike Falcon für Bedrohungsinformationen anzeigen** . Klicken Sie auf die Links, um sie anzuzeigen [Bedrohungsinformationen](#) bei CrowdStrike Falcon.
- Wählen **Links zu CrowdStrike für Geräte anzeigen, auf denen Falcon-Software installiert ist**. Geräte müssen lokal sein und eine MAC-Adresse haben. Links erscheinen auf der [Seite „Geräteübersicht“](#) für CrowdStrike-Geräte.
- Wählen **Ermöglichen Sie es Benutzern, CrowdStrike-Geräte vor Erkennungen in Reveal (x) 360 zu schützen**. (Erfordert Lese- und Schreibzugriff auf Hosts). Eine Option erscheint [die Eindämmung von CrowdStrike-Geräten einleiten](#) das sind Teilnehmer an einer Sicherheitserkennung. Benutzern muss der Zugriff über die globale Richtlinie für Erkennungszugriffskontrolle gewährt werden und sie müssen über vollständige Schreibrechte oder höher verfügen, um die Eingrenzung einleiten zu können.

6. klicken **Speichern**.