Integrieren Sie Reveal (x) 360 mit CrowdStrike

Veröffentlicht: 2023-10-24

Integrieren Sie ExtraHop Reveal (x) 360 mit CrowdStrike, um mehr Transparenz und Bedrohungsinformationen über Ihre Geräte zu erhalten.

Anforderungen an das System

ExtraHop Reveal (x) 360

- Ihr Benutzerkonto muss über Rechte auf Reveal (x) 360 für System- und Zugriffsadministration oder 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 Gerät Containment 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 in Ihrer CrowdStrike-API-Client-ID, Ihrem geheimen Client-Schlüssel 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 LESEberechtigungen für Indikatoren (Falcon X) enthalten, um Integrationsoptionen für die Anzeige von Links zu CrowdStrike-Geräten oder den Import von Bedrohungsinformationen aus CrowdStrike Falcon zu ermöglichen.
- Der Umfang des CrowdStrike-API-Clients muss READ- und WRITE-Berechtigungen für Hosts enthalten, um die Integrationsoption für die Geräteeindämmung zu aktivieren.

Konfiguration der CrowdStrike-Integration

1. Melden Sie sich beim Reveal (x) 360-System an.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **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-Regionsendpunkt 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 insgesamt nicht mehr als 50.000 Indikatoren aus CrowdStrike importieren.

- Wählen **Threat Intelligence für IP-Adressen aus CrowdStrike Falcon importieren**. Im Reveal (x) 360-System erscheint ein visueller Hinweis für jede Aktivität, die mit einem Eintrag im CrowdStrike übereinstimmt Sammlung von Bedrohungen.
- Wählen **Import von Bedrohungsinformationen für Domains und Hostnamen aus CrowdStrike Falcon**. Im Reveal (x) 360-System erscheint ein visueller Hinweis für jede Aktivität, die mit einem Eintrag in der CrowdStrike-Bedrohungssammlung übereinstimmt.
- Wählen **Links zu CrowdStrike für Geräte anzeigen, auf denen die Falcon-Software installiert ist**. Geräte müssen lokal sein und eine MAC-Adresse haben. Links erscheinen auf der Seite „ Geräteübersicht“ für CrowdStrike-Geräte.
- Wählen **Benutzern ermöglichen, CrowdStrike-Geräte aus Erkennungen in Reveal (x) 360 einzudämmen**. (Erfordert Lese- und Schreibzugriff auf Hosts). Eine Option erscheint für Eindämmung von CrowdStrike-Geräten einleiten das sind Teilnehmer an einer Sicherheitserkennung. Benutzern muss der Zugriff über die globale Richtlinie für Erkennungszugriffskontrolle gewährt werden und über vollständige Schreibrechte oder höher verfügen, um die Eindämmung zu initiieren.

6. klicken **Speichern**.