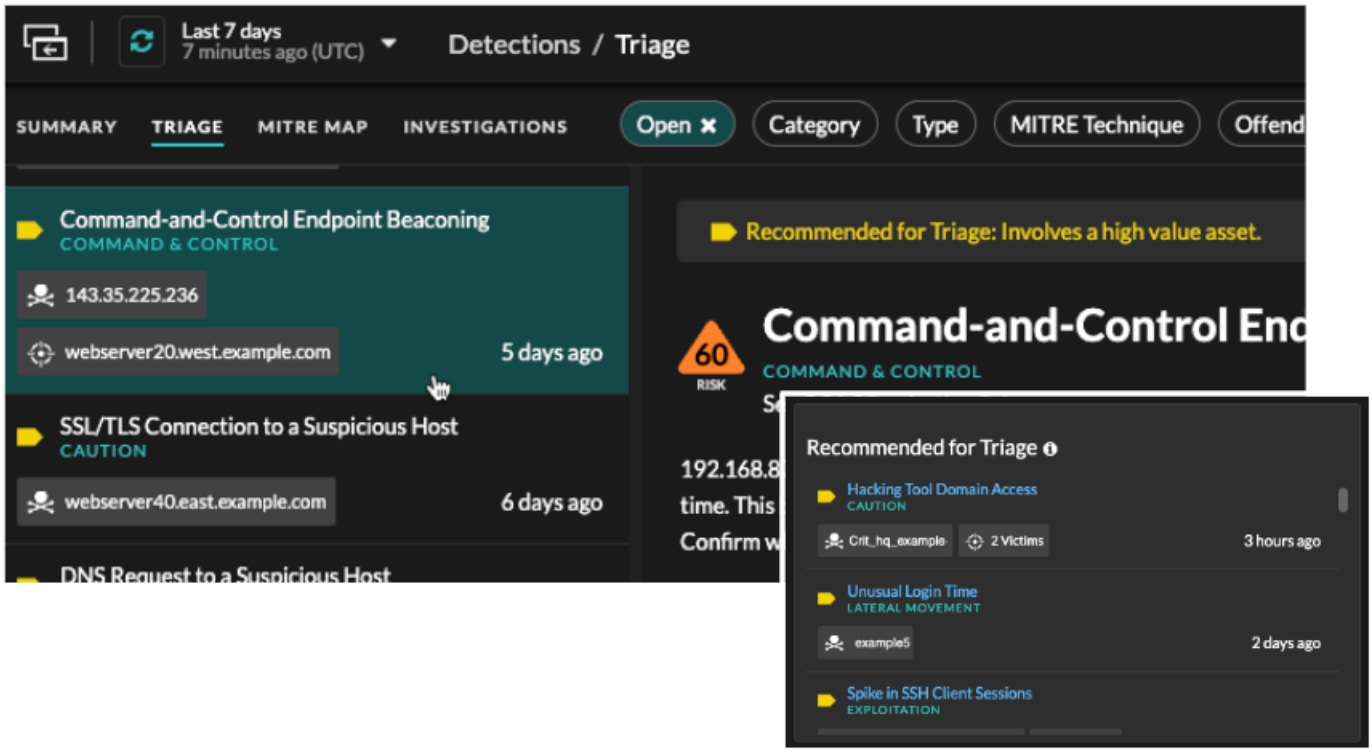
Was ist neu

Veröffentlicht: 2023-11-13

Während Versionshinweise bieten einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.4.

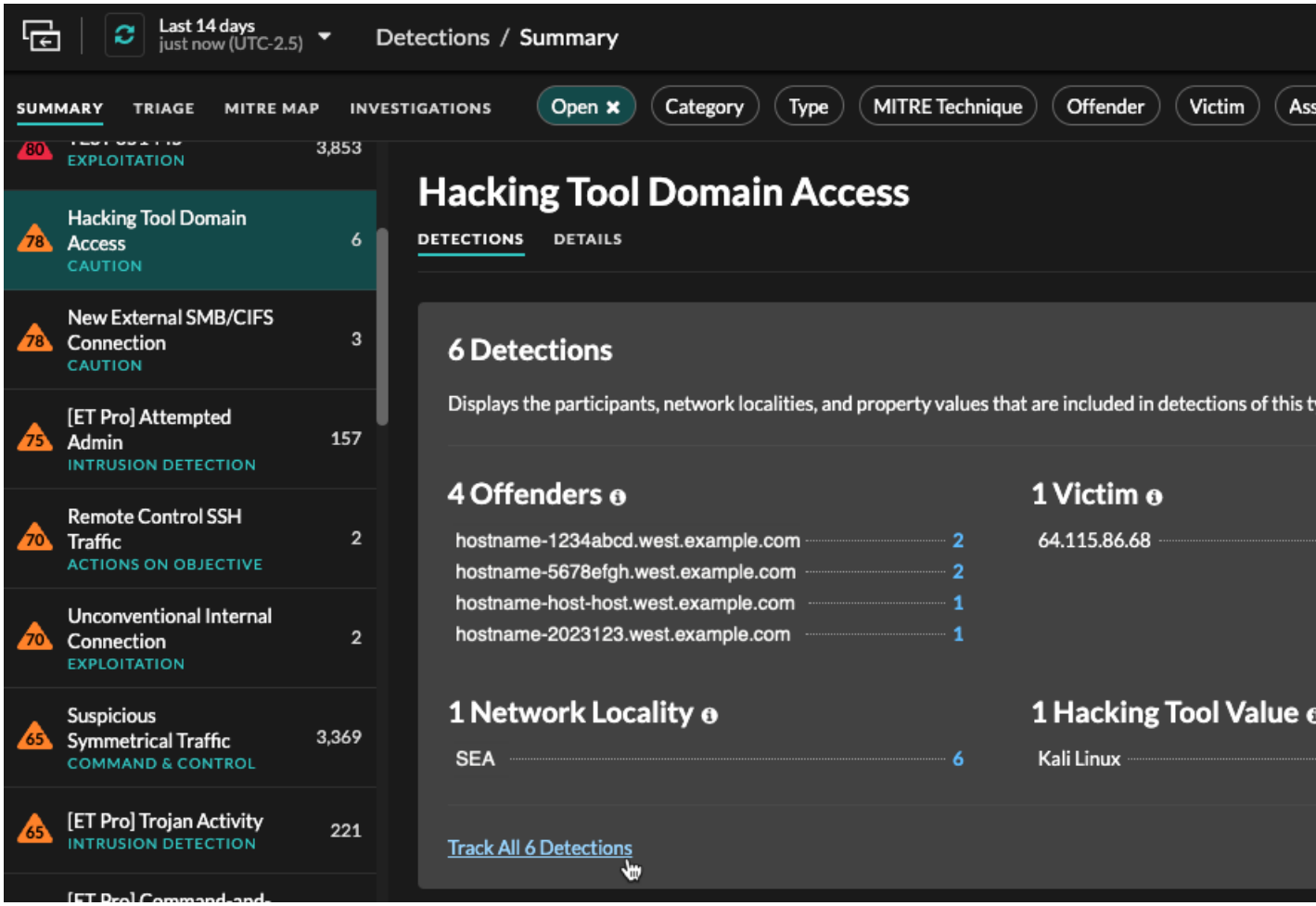
Erkennung und Triage

Das ExtraHop-System empfiehlt jetzt Erkennungen für die Triage auf der Grundlage einer Kontextanalyse verschiedener Faktoren in Ihrer Umgebung. Empfehlungen sind hervorgehoben in Triage auf der Erkennungsseite und auf der Überblick über die Sicherheit Seite.



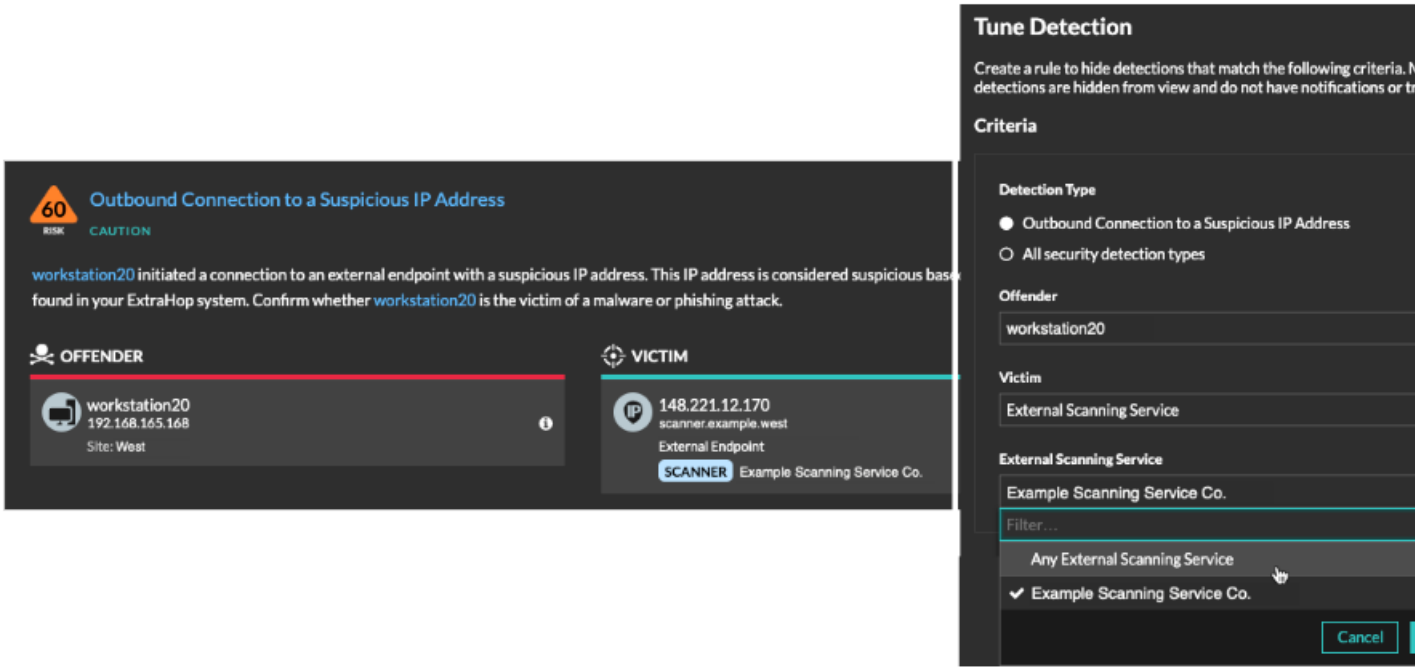
Zusammenfassung der Erkennung

In der Übersichtsansicht auf der Seite Erkennungen werden Informationen zusammengefasst nach Erkennungstyp oder Quelle und ermöglicht es Ihnen stimmen und Spur mehrere Erkennungen gleichzeitig.



Externe Scandienste

ExtraHop identifiziert jetzt externe Scandienste und kennzeichnet sie als Teilnehmer an Erkennungen. Du kannst Tuning-Regeln erstellen für einen bestimmten externen Scandienst oder blenden Sie alle Erkennungen aus, die einen externen Scandienst betreffen.



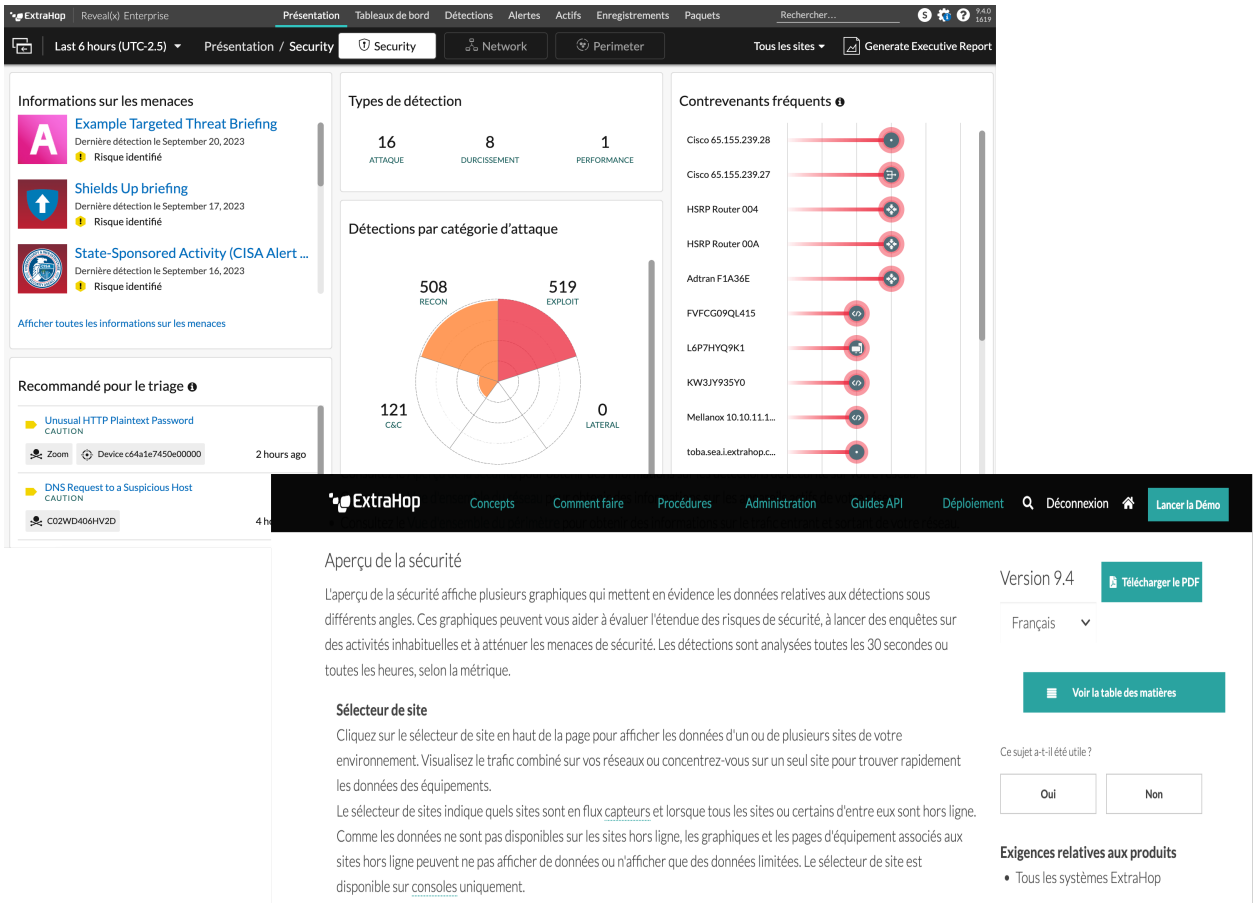
Geolokalisierungskarte

Der Tab Länder wurde auf der Seite Perimeter Overview in Geolocation umbenannt und die Halo-Visualisierung durch eine interaktive Weltkarte ersetzt. Die Geolokalisierungskarte zeigt den Verkehr zwischen internen Endpunkten und geografischen Standorten an, die auf der Karte in einer kontrastierenden Farbe hervorgehoben sind. Die Intensität der kontrastierenden Farbe steht für das Verkehrsaufkommen an dieser Geolokation. Klicken Sie auf eine hervorgehobene Geolokalisierung auf der Karte, um die Gesamtmenge des eingehenden oder ausgehender Datenverkehr im Zusammenhang mit verbundenen internen Endpunkten anzuzeigen.


Last 6 hours
Overview / Perimeter
Secur
CLOUD SERVICES
GEOLOCATION
LARGE UPLOADS

Auswahl der Sprache

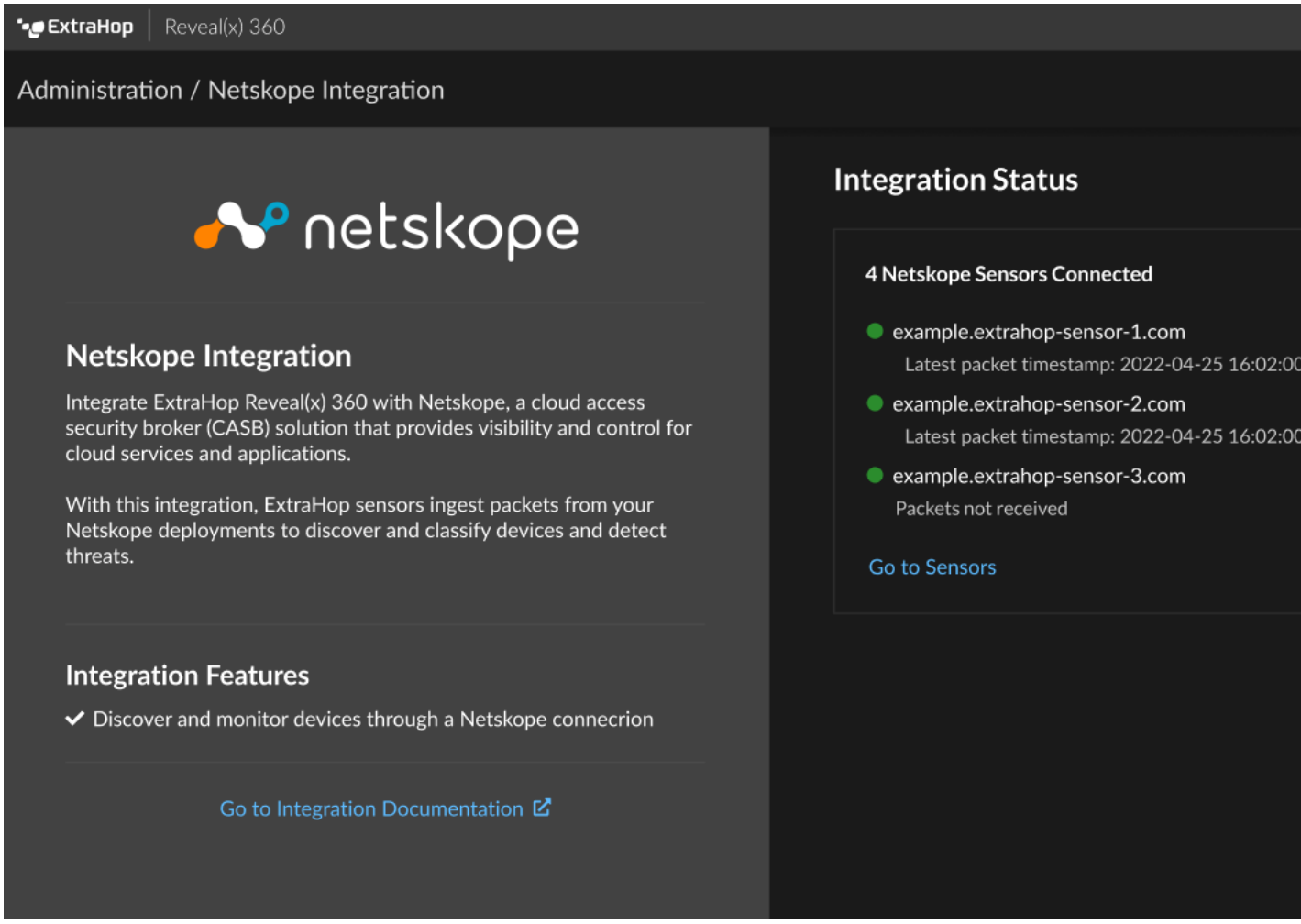
Das ExtraHop-System ermöglicht Ihnen zeigt Französisch oder Deutsch in ausgewählten Bereichen der Benutzeroberfläche an und in der Dokumentation.



Netskope-Integration

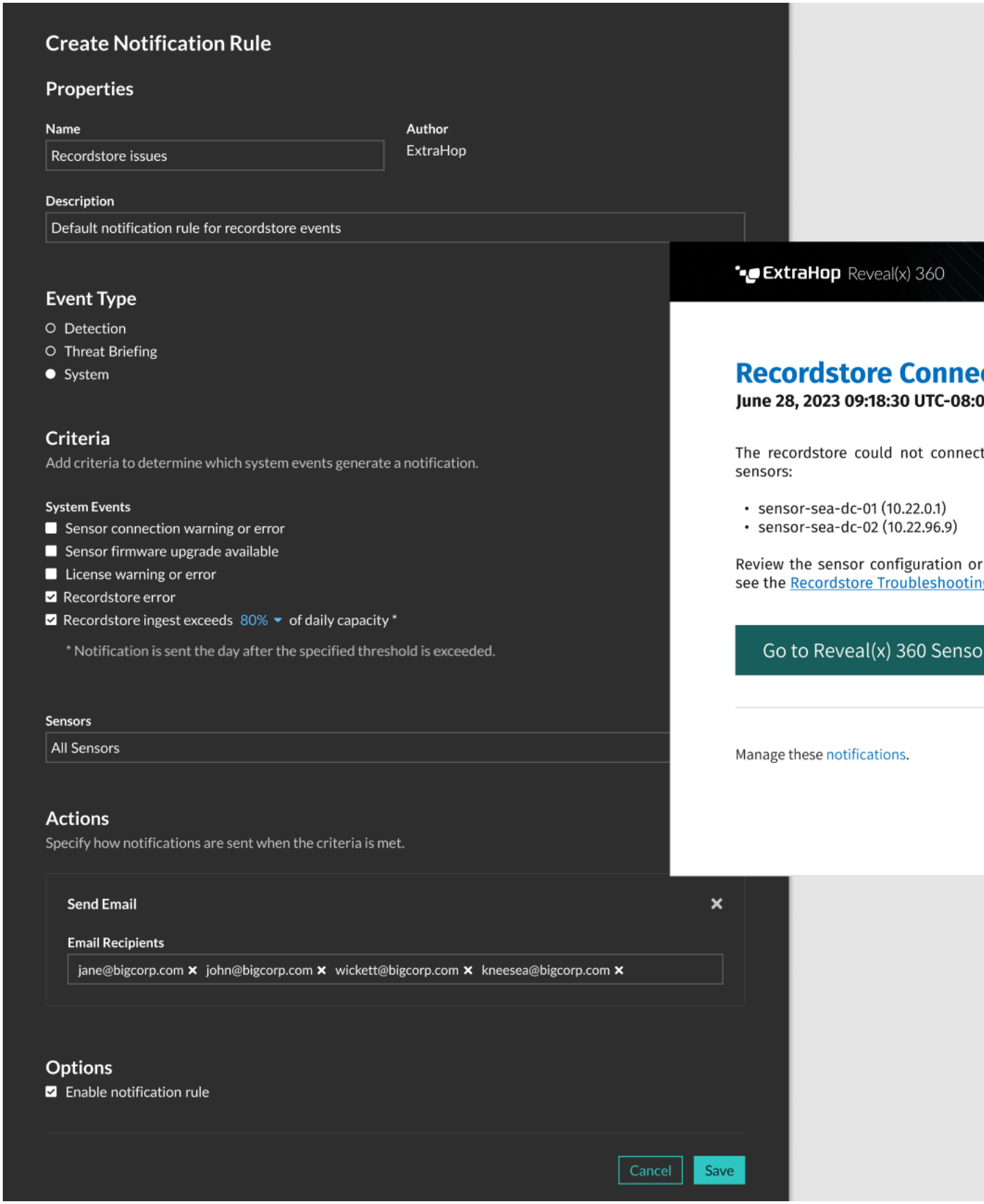
Hinweis Die Reveal (x) -Integration mit Netskope Intelligent Security Service Edge (SSE) steht derzeit nur Teilnehmern des Netskope Cloud TAP Early Access Programms zur Verfügung. Wenn Sie mehr über diese Integration erfahren und benachrichtigt werden möchten, sobald sie öffentlich verfügbar ist, wenden Sie sich bitte an Ihr ExtraHop-Kundenbetreuungsteam.

Diese Integration ermöglicht Ihnen konfigurieren Sie ExtraHop-Sensoren so, dass sie Pakete aus Ihrer Netskope-Lösung aufnehmen um Bedrohungen zu erkennen, Geräte zu entdecken und zu überwachen und Einblicke in den Datenverkehr zu gewinnen. Reveal (x) 360-Benutzer können zur Netskope-Integrationsseite navigieren, um den Verbindungsstatus der Sensor einzusehen.



Enthüllen (x) 360

Mit dem ExtraHop-System können Sie jetzt eine Regel für Systembenachrichtigungen erstellen um eine Empfängerliste per E-Mail zu versenden, wenn der Recordstore keine Verbindung zu einem Sensor herstellen kann, um Datensätze zu empfangen, und wenn die Verbindung wiederhergestellt ist.


Create Notification Rule
Properties
Name
Recordstore issues
Author
ExtraHop
Description
Default notification rule for recordstore events
Event Type
Detection
Threat Briefing
System
Criteria
Add criteria to determine which system events generate a notification.
System Events
Sensor connection warning or error
Sensor firmware upgrade available
License warning or error
Recordstore error
Recordstore ingest exceeds 80% of daily capacity *
* Notification is sent the day after the specified threshold is exceeded.
Sensors
All Sensors
Actions
Specify how notifications are sent when the criteria is met.
Send Email
Email Recipients
jane@bigcorp.com
john@bigcorp.com
wickett@bigcorp.com
kneesea@bigcorp.com
Options
Enable notification rule
Cancel
Save
ExtraHop Reveal(x) 360
Recordstore Connec
June 28, 2023 09:18:30 UTC-08:0
The recordstore could not connect
sensors:
sensor-sea-dc-01 (10.22.0.1)
sensor-sea-dc-02 (10.22.96.9)
Review the sensor configuration or
see the Recordstore Troubleshootin
Go to Reveal(x) 360 Senso
Manage these notifications.

Wenn Sie eine hinzugefügt haben benutzerdefinierter Identitätsanbieter, sendet das ExtraHop-System automatisch Benachrichtigungen über den Ablauf des Identity Provider-Zertifikats (IdP) an alle Benutzer mit System- und Zugriffsadministrationsrechten. E-Mails werden 1 Monat, 2 Wochen und 1 Woche vor dem Ablaufdatum des Zertifikats gesendet.