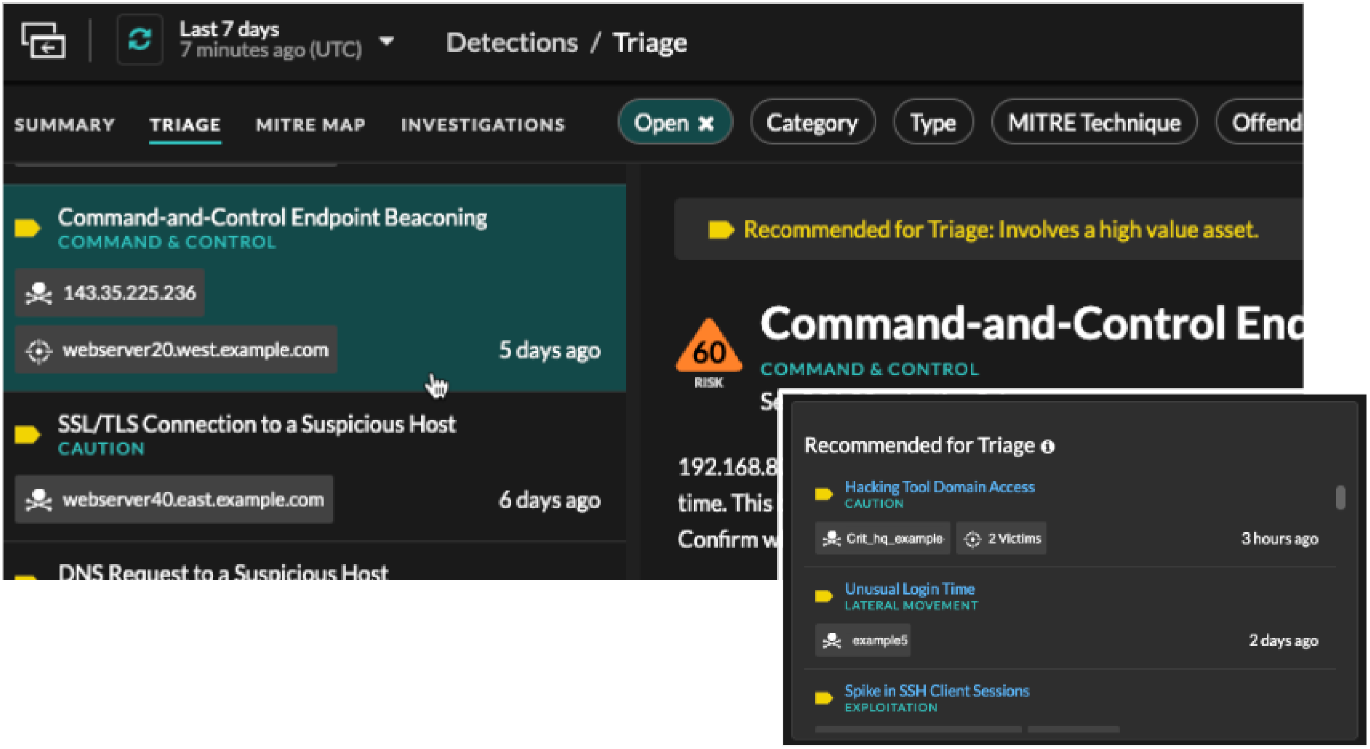
What's New

Published: 2023-10-26

While release notes provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.4.

Detection Triage

The ExtraHop system now recommends detections for triage based on contextual analysis of several factors in your environment. Recommendations are highlighted in Triage on the Detections page and on the Security Overview page.



Command-and-Control Endpoint Beaconing
COMMAND & CONTROL
143.35.225.236
webserver20.west.example.com 5 days ago

SSL/TLS Connection to a Suspicious Host
CAUTION
webserver40.east.example.com 6 days ago

DNS Request to a Suspicious Host

Recommended for Triage: Involves a high value asset.

Command-and-Control End
COMMAND & CONTROL
192.168.8
time. This
Confirm w

Recommended for Triage

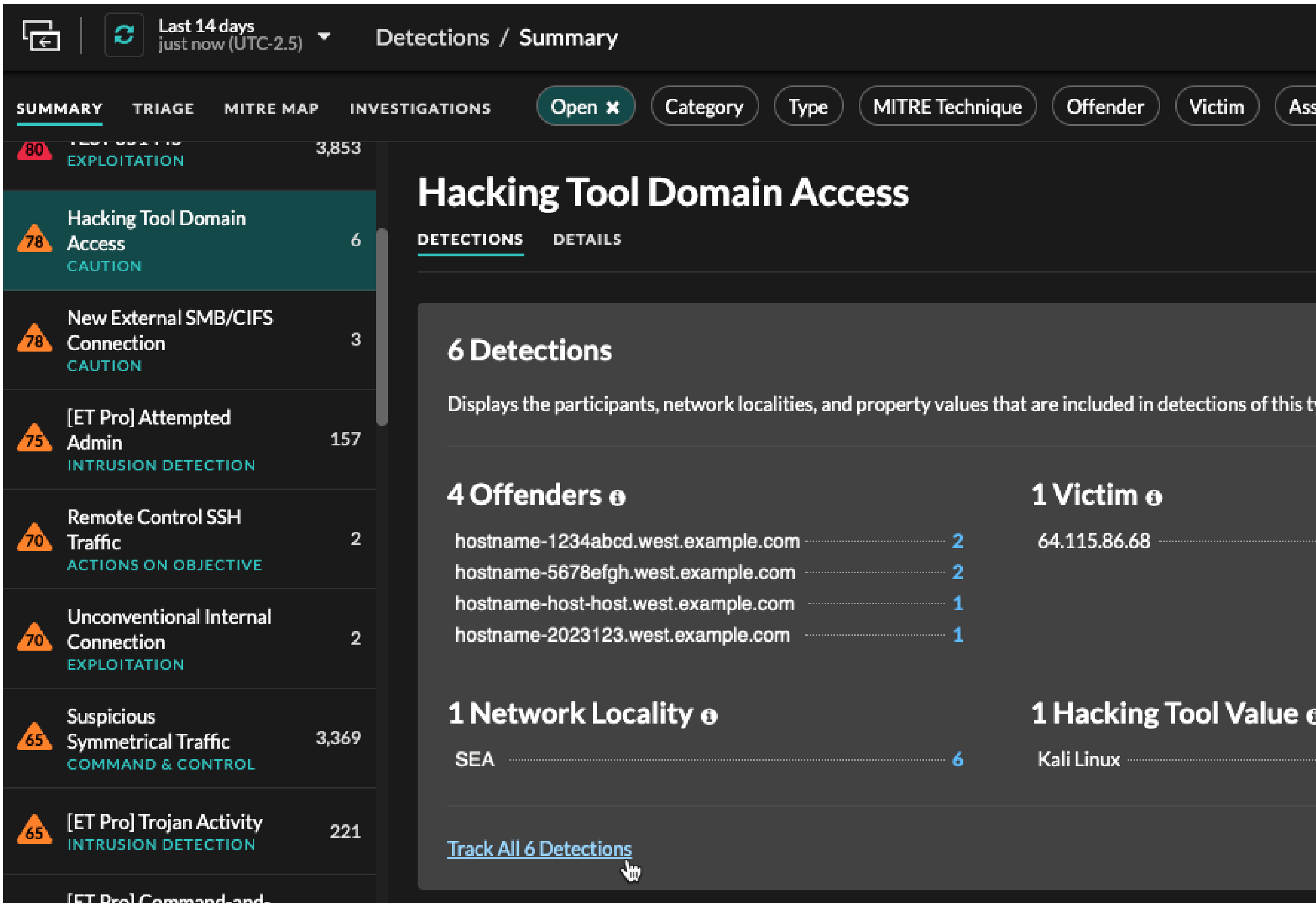
Hacking Tool Domain Access
CAUTION
Crit_hq_example 2 Victims 3 hours ago

Unusual Login Time
LATERAL MOVEMENT
example5 2 days ago

Spike in SSH Client Sessions
EXPLOITATION

Detection Summary

The Summary view on the Detections page aggregates information by detection type or source and enables you to tune and track multiple detections at once.



Displays the participants, network localities, and property values that are included in detections of this t

4 Offenders	
hostname-1234abcd.west.example.com	2
hostname-5678efgh.west.example.com	2
hostname-host-host.west.example.com	1
hostname-2023123.west.example.com	1

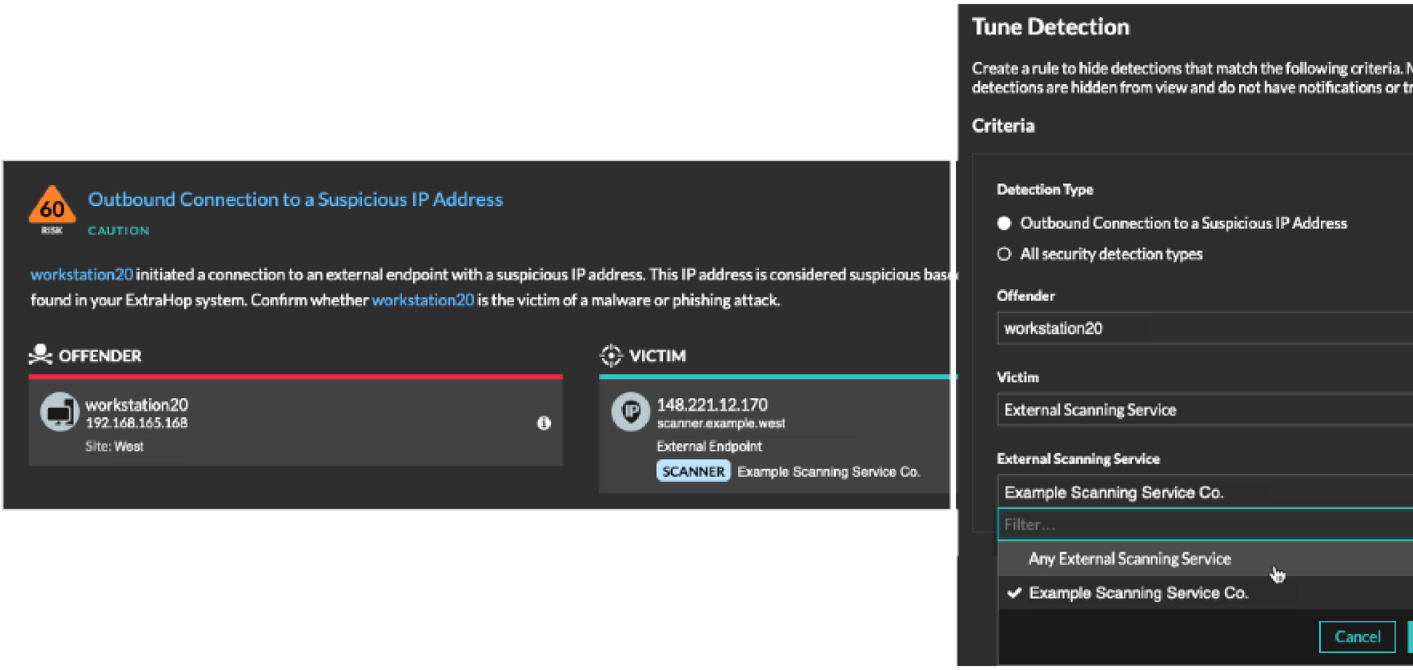
1 Victim
64.115.86.68

1 Network Locality	
SEA	6

1 Hacking Tool Value
Kali Linux

External Scanning Services

ExtraHop now identifies external scanning services and flags them as participants in detections. You can create tuning rules for a specific external scanning service or hide all detections involving an external scanning service.



60 RISK

Outbound Connection to a Suspicious IP Address

CAUTION

workstation20 initiated a connection to an external endpoint with a suspicious IP address. This IP address is considered suspicious bas found in your ExtraHop system. Confirm whether workstation20 is the victim of a malware or phishing attack.

Tune Detection

Create a rule to hide detections that match the following criteria. N detections are hidden from view and do not have notifications or tr

Criteria

Detection Type

● Outbound Connection to a Suspicious IP Address

○ All security detection types

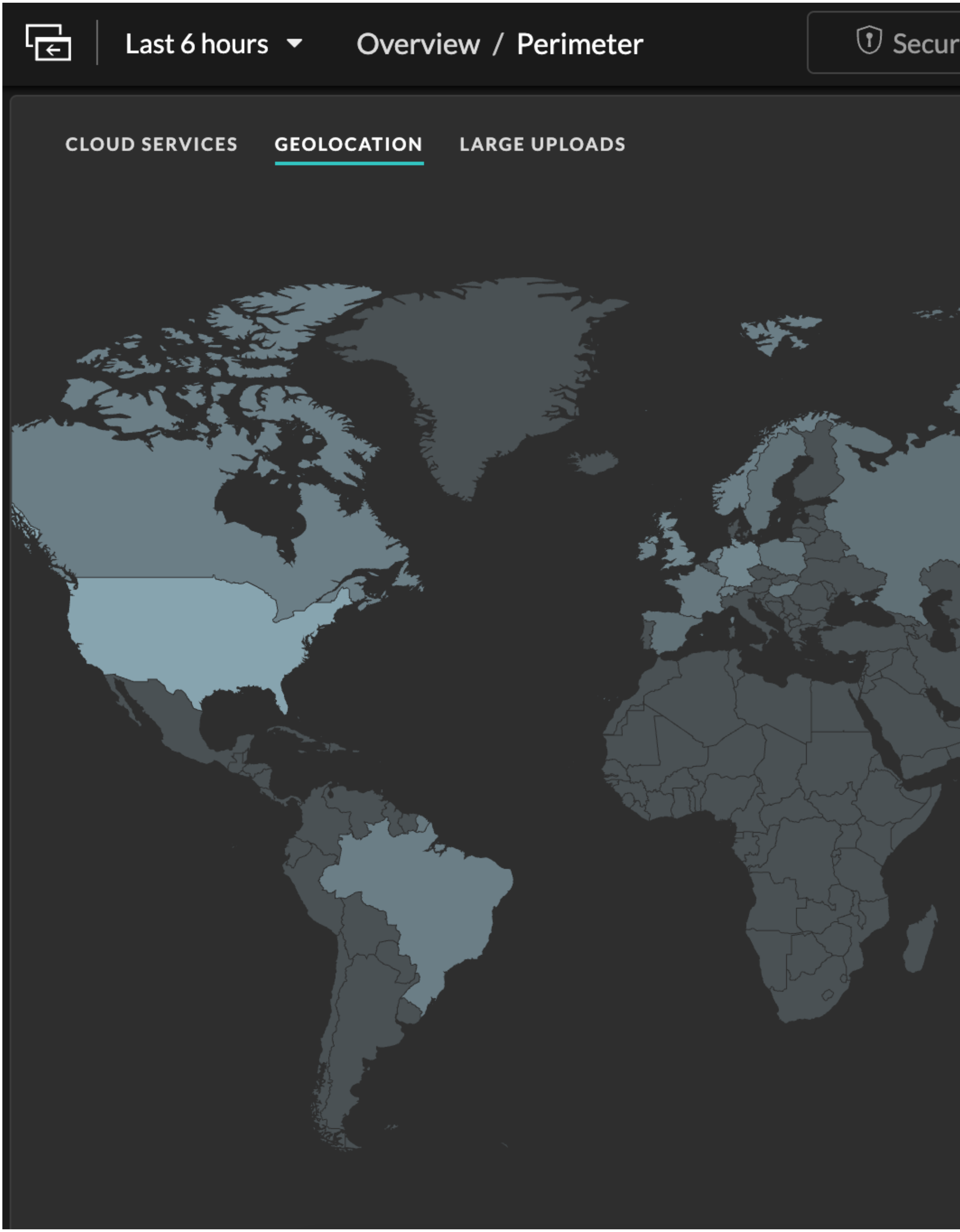
Offender: workstation20

Victim: External Scanning Service

External Scanning Service: Example Scanning Service Co.

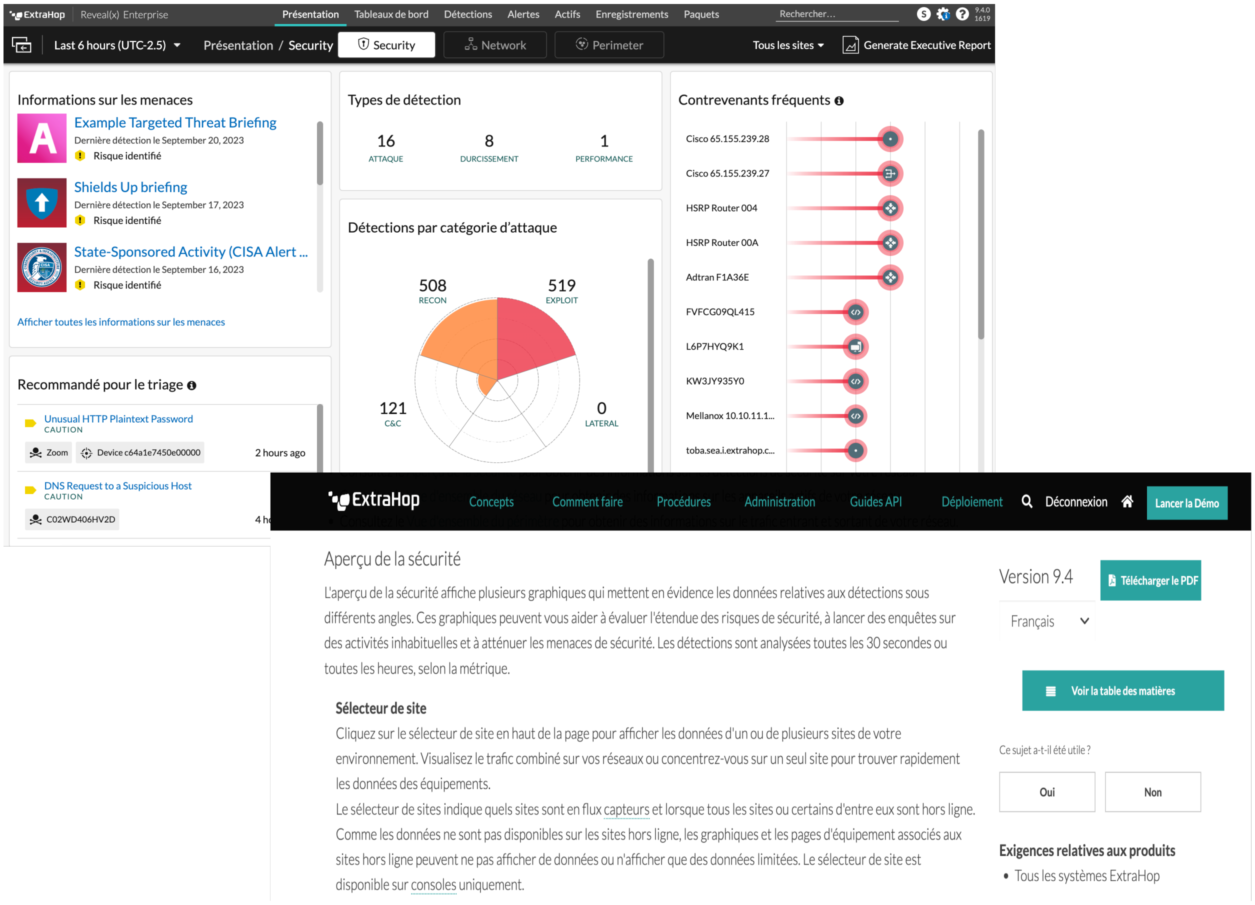
Geolocation Map

Renamed the Countries tab to Geolocation on the Perimeter Overview page and replaced the halo visualization with an interactive world map. The Geolocation map indicates traffic between internal endpoints and geographic locations, which are highlighted in a contrasting color on the map. The intensity of the contrasting color represents the amount of traffic at that geolocation. Click a highlighted geolocation from the map to view the total amount of inbound or outbound traffic associated with connected internal endpoints.


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

Language Selection

The ExtraHop system enables you to display French or German in select areas of the user interface and in the documentation.



Aperçu de la sécurité

L'aperçu de la sécurité affiche plusieurs graphiques qui mettent en évidence les données relatives aux détections sous différents angles. Ces graphiques peuvent vous aider à évaluer l'étendue des risques de sécurité, à lancer des enquêtes sur des activités inhabituelles et à atténuer les menaces de sécurité. Les détections sont analysées toutes les 30 secondes ou toutes les heures, selon la métrique.

Sélecteur de site

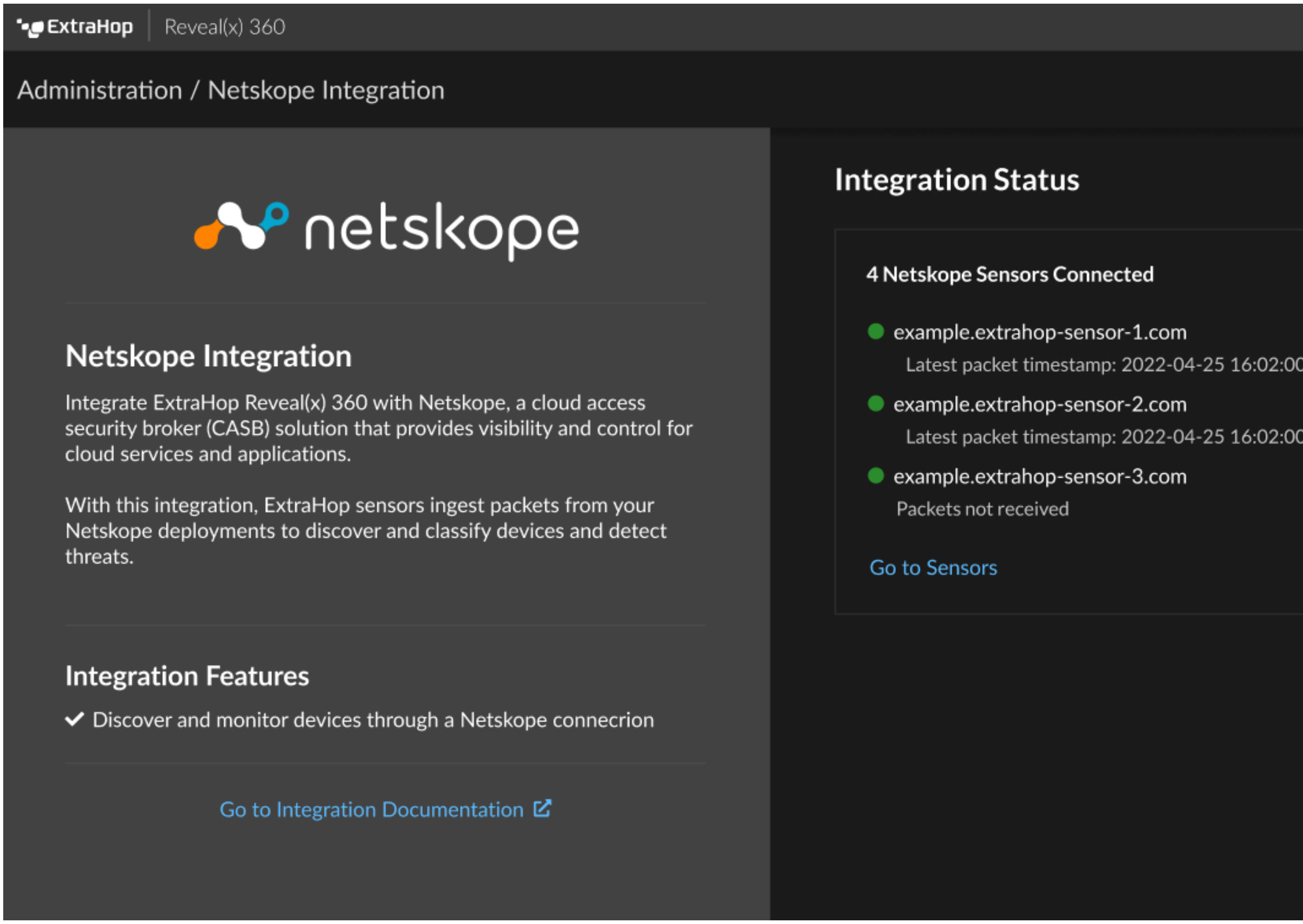
Cliquez sur le sélecteur de site en haut de la page pour afficher les données d'un ou de plusieurs sites de votre environnement. Visualisez le trafic combiné sur vos réseaux ou concentrez-vous sur un seul site pour trouver rapidement les données des équipements.

Le sélecteur de sites indique quels sites sont en flux capteurs et lorsque tous les sites ou certains d'entre eux sont hors ligne. Comme les données ne sont pas disponibles sur les sites hors ligne, les graphiques et les pages d'équipement associés aux sites hors ligne peuvent ne pas afficher de données ou n'afficher que des données limitées. Le sélecteur de site est disponible sur consoles uniquement.

Netskope Integration

Note: The Reveal(x) integration with Netskope Intelligent Security Service Edge (SSE) is currently only available to Netskope Cloud TAP Early Access Program participants. If you would like to learn more about this integration and be notified as soon as it is publicly available, please reach out to your ExtraHop account team.

This integration enables you to configure ExtraHop sensors to ingest packets from your Netskope solution to detect threats, discover and monitor devices, and gain insight into traffic. Reveal(x) 360 users can navigate to the Netskope integration page to view sensor connection status.



ExtraHop | Reveal(x) 360

Administration / Netskope Integration

Netskope Integration

Integrate ExtraHop Reveal(x) 360 with Netskope, a cloud access security broker (CASB) solution that provides visibility and control for cloud services and applications.

With this integration, ExtraHop sensors ingest packets from your Netskope deployments to discover and classify devices and detect threats.

Integration Features

✓ Discover and monitor devices through a Netskope connecrion

Go to Integration Documentation

Integration Status

4 Netskope Sensors Connected

● example.extrahop-sensor-1.com
Latest packet timestamp: 2022-04-25 16:02:00

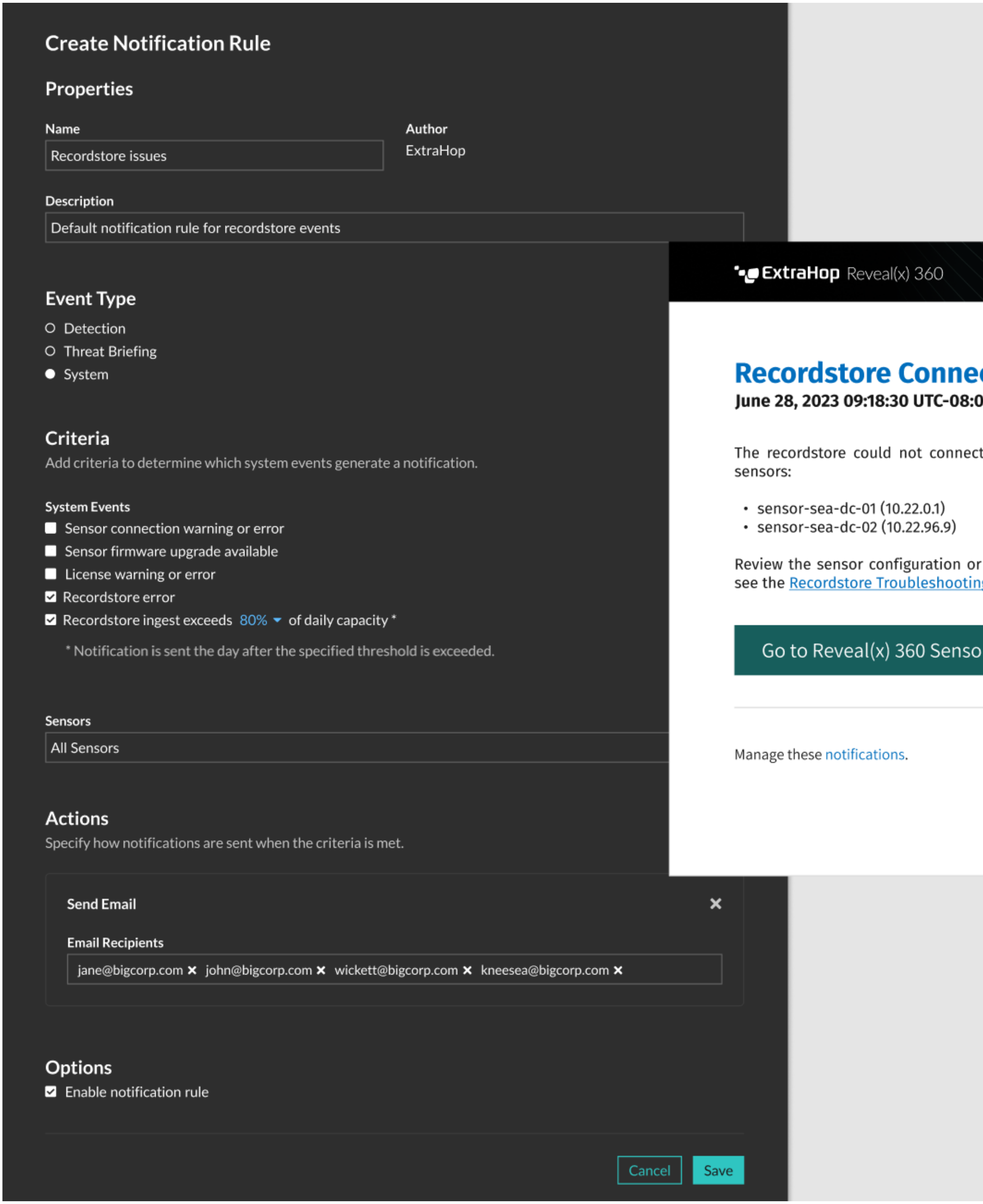
● example.extrahop-sensor-2.com
Latest packet timestamp: 2022-04-25 16:02:00

● example.extrahop-sensor-3.com
Packets not received

Go to Sensors

Reveal(x) 360

The ExtraHop system now enables you to create a system notification rule to email a recipient list whenever the recordstore cannot connect to a sensor to receive records and when the connection is restored.



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

ExtraHop Reveal(x) 360

Recordstore Conne

June 28, 2023 09:18:30 UTC-08:0

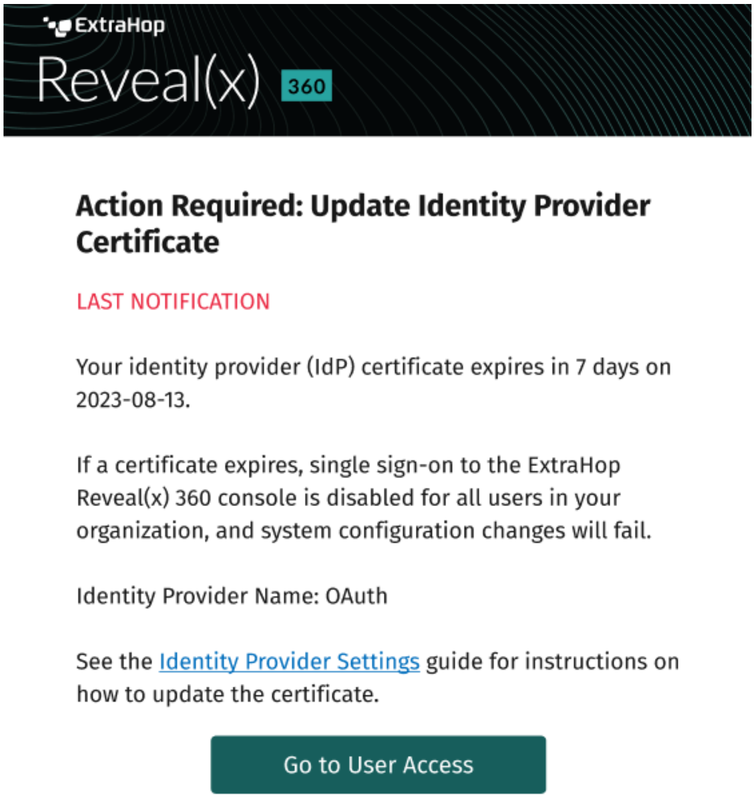
The recordstore could not connect
sensors:

- 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

Manage these notifications.

If you have added a custom identity provider, the ExtraHop system automatically sends identity provider (IdP) certificate expiration notifications to all users with System and Access Administration privileges. Emails are sent 1 month, 2 weeks, and 1 week prior to the certificate expiration date.



Action Required: Update Identity Provider Certificate

LAST NOTIFICATION

Your identity provider (IdP) certificate expires in 7 days on 2023-08-13.

If a certificate expires, single sign-on to the ExtraHop Reveal(x) 360 console is disabled for all users in your organization, and system configuration changes will fail.

Identity Provider Name: OAuth

See the Identity Provider Settings guide for instructions on how to update the certificate.