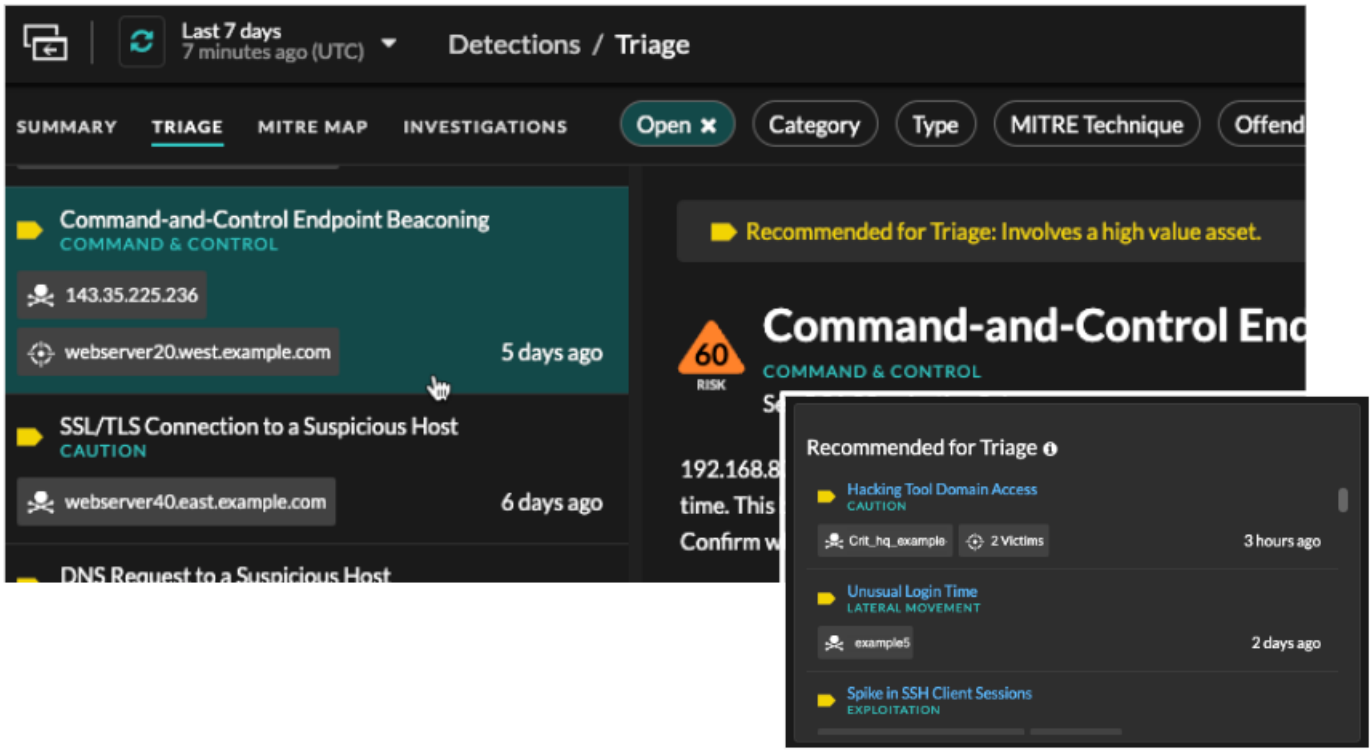
Quoi de neuf

Publié: 2023-11-14

Tandis que notes de version pour avoir une vue complète de nos mises à jour, voici un aperçu des fonctionnalités les plus intéressantes d'ExtraHop 9.4.

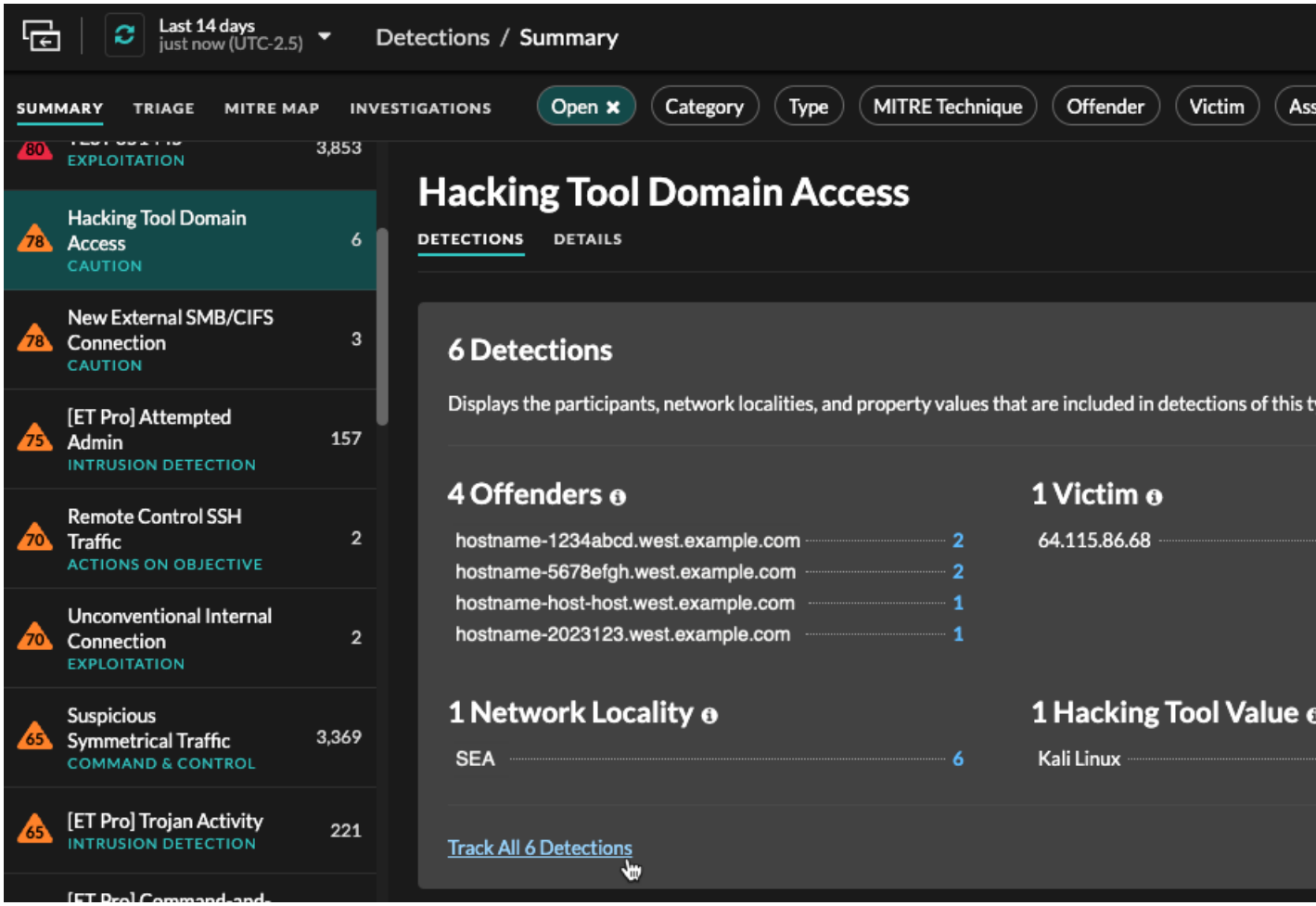
Détection et triage

Le système ExtraHop recommande désormais des détections pour le triage sur la base d'une analyse contextuelle de plusieurs facteurs de votre environnement. Les recommandations sont mises en évidence dans Triage sur la page Détections et sur le Aperçu de la sécurité page.



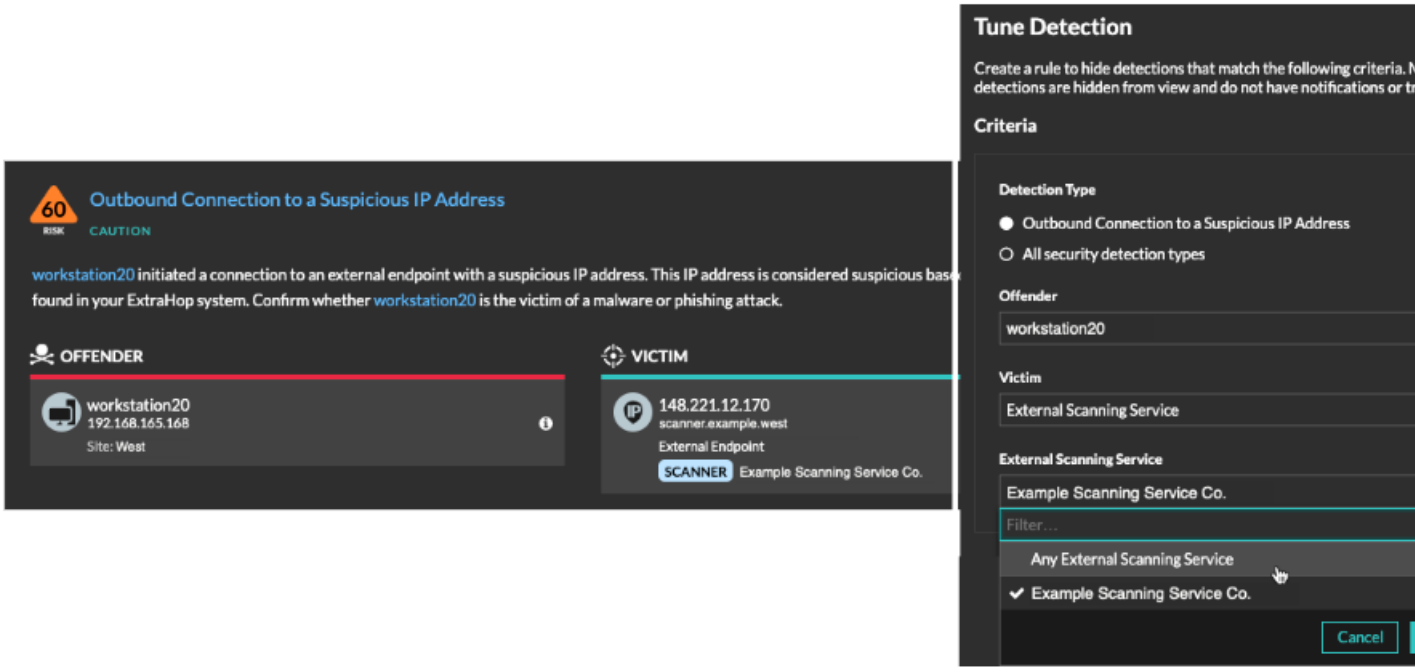
Résumé des détections

La vue récapitulative de la page Détections regroupe les informations par type de détection ou par source et vous permet de syntoniser et piste plusieurs détections à la fois.



Services de numérisation externes

ExtraHop identifie désormais les services de numérisation externes et les signale comme participants aux détections. Tu peux créer des règles de réglage pour un service d'analyse externe spécifique ou masquez toutes les détections impliquant un service de numérisation externe.



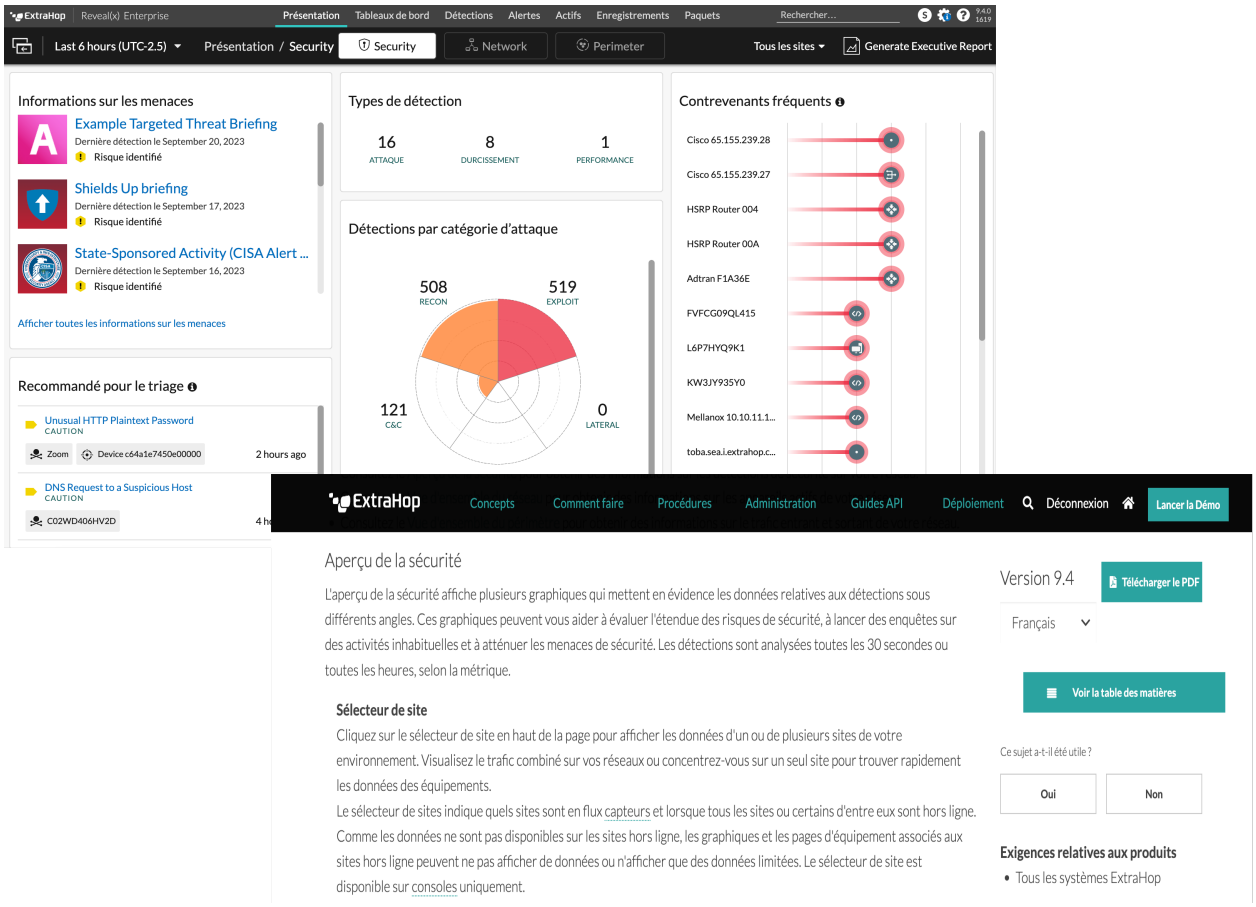
Carte de géolocalisation

Sur la page d'aperçu du périmètre, l'onglet Pays a été renommé en Géolocalisation et la visualisation du halo a été remplacée par une carte du monde interactive. Le Carte de géolocalisation indique le trafic entre les points de terminaison internes et les emplacements géographiques, qui sont surlignés dans une couleur contrastante sur la carte. L'intensité de la couleur contrastante représente le volume de trafic à cette géolocalisation. Cliquez sur une géolocalisation surlignée sur la carte pour afficher le volume total de trafic entrant ou sortant associé aux points de terminaison internes connectés.


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

Sélection de la langue

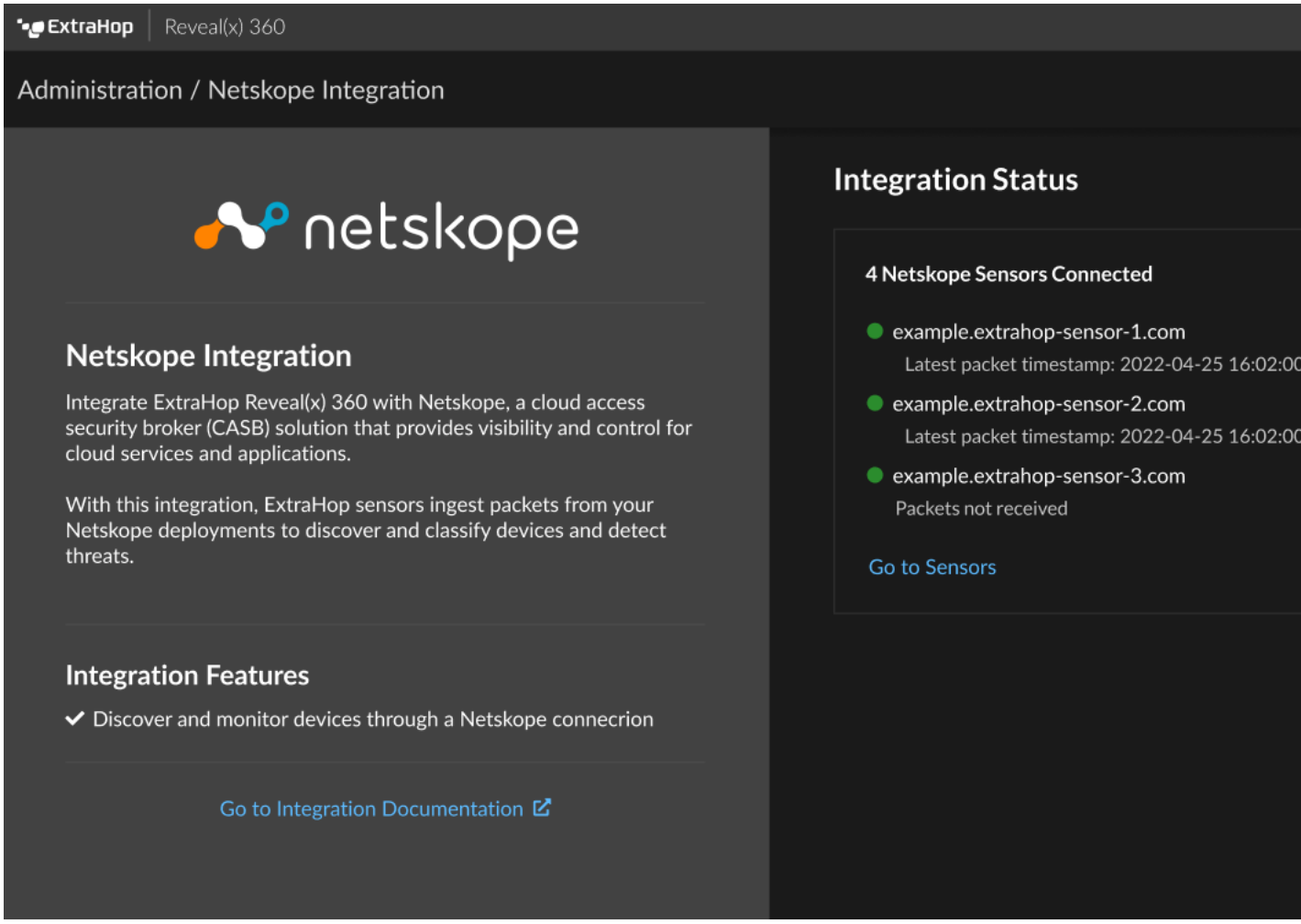
Le système ExtraHop vous permet de afficher le français ou l' allemand dans certaines zones de l'interface utilisateur et dans la documentation.



Intégration à Netskope

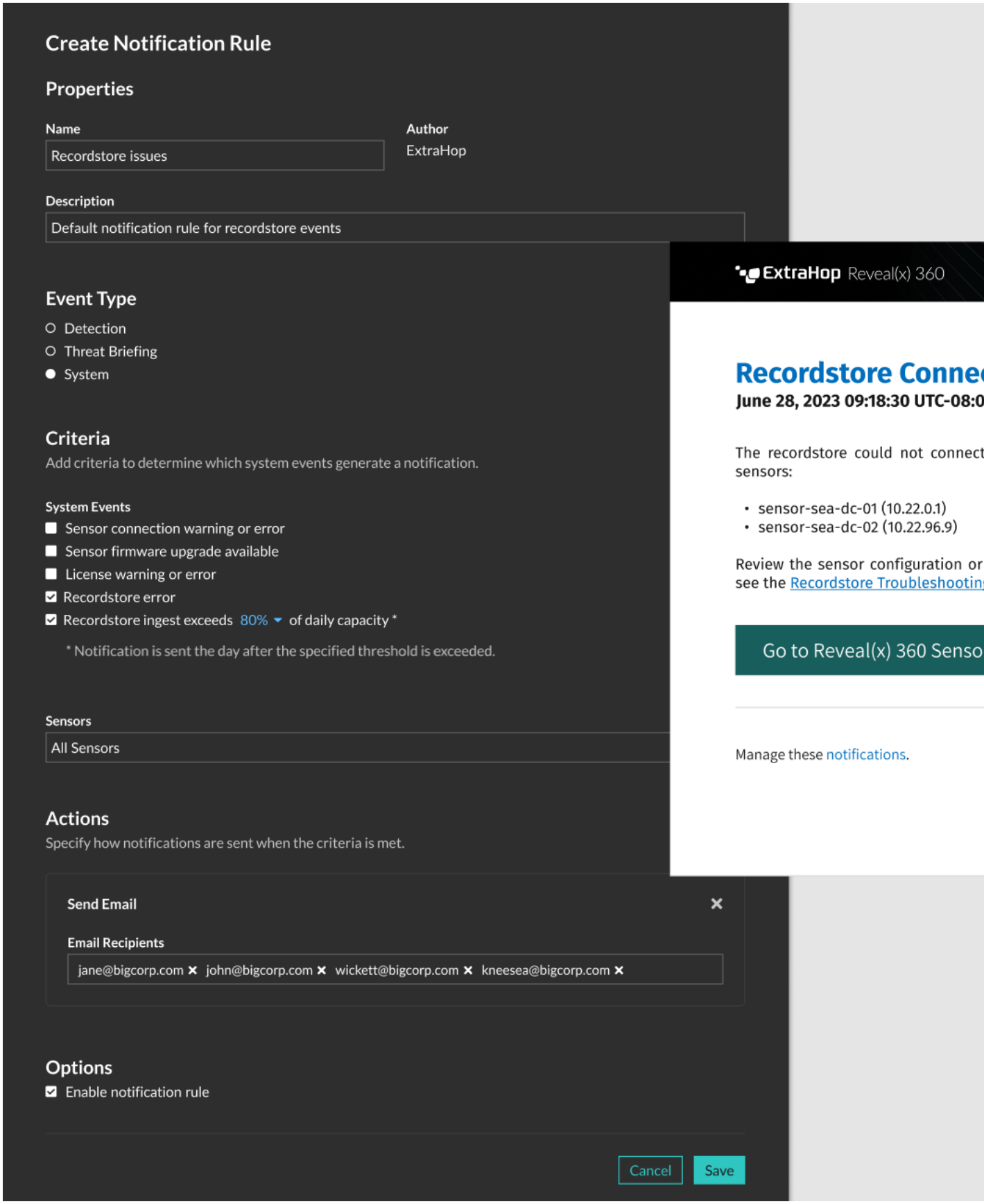
Note: L'intégration de Reveal (x) avec Netskope Intelligent Security Service Edge (SSE) n'est actuellement disponible que pour les participants au programme Netskope Cloud TAP Early Access. Si vous souhaitez en savoir plus sur cette intégration et être averti dès qu'elle sera disponible au public, veuillez contacter l'équipe de votre compte ExtraHop.

Cette intégration vous permet de configurer des capteurs ExtraHop pour ingérer des paquets depuis votre solution Netskope pour détecter les menaces, découvrir et surveiller les appareils, et obtenir un aperçu du trafic. Les utilisateurs de Reveal (x) 360 peuvent accéder à la page d'intégration de Netskope pour voir l'état de connexion des sondes.



Révéler (x) 360

Le système ExtraHop vous permet désormais de créer une règle de notification système pour envoyer une liste de destinataires par e-mail chaque fois que l' espace de stockage des enregistrements ne peut pas se connecter à une sonde pour recevoir des enregistrements et lorsque la connexion est rétablie.


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.

Si vous avez ajouté un fournisseur d'identité personnalisé, le système ExtraHop envoie automatiquement des notifications d'expiration des certificats du fournisseur d'identité (IdP) à tous les utilisateurs disposant de privilèges d' administration du système et des accès. Les e-mails sont envoyés 1 mois, 2 semaines et 1 semaine avant la date d'expiration du certificat.