

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.

The screenshot displays the ExtraHop Detections/Triage interface. The main view shows a list of detections under the 'TRIAGE' tab. A 'Command-and-Control Endpoint Beacons' detection is highlighted, showing IP 143.35.225.236 and host webserver20.west.example.com, detected 5 days ago. Below it is an 'SSL/TLS Connection to a Suspicious Host' detection with IP 192.168.8.100 and host webserver40.east.example.com, detected 6 days ago. A 'Recommended for Triage' overlay is visible, listing 'Hacking Tool Domain Access' (3 hours ago), 'Unusual Login Time' (2 days ago), and 'Spike in SSH Client Sessions'. The interface includes filters for Category, Type, MITRE Technique, and Offender.

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.

🏠 🔄 Last 14 days just now (UTC-2.5) ▼ Detections / Summary

SUMMARY TRIAGE MITRE MAP INVESTIGATIONS Open ✕ Category Type MITRE Technique Offender Victim Ass

Score	Category	Count
80	EXPLOITATION	3,853
78	Hacking Tool Domain Access CAUTION	6
78	New External SMB/CIFS Connection CAUTION	3
75	[ET Pro] Attempted Admin INTRUSION DETECTION	157
70	Remote Control SSH Traffic ACTIONS ON OBJECTIVE	2
70	Unconventional Internal Connection EXPLOITATION	2
65	Suspicious Symmetrical Traffic COMMAND & CONTROL	3,369
65	[ET Pro] Trojan Activity INTRUSION DETECTION	221

Hacking Tool Domain Access

DETECTIONS DETAILS

6 Detections

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

4 Offenders	1 Victim
hostname-1234abcd.west.example.com 2	64.115.86.68 1
hostname-5678efgh.west.example.com 2	
hostname-host-host.west.example.com 1	
hostname-2023123.west.example.com 1	
1 Network Locality	1 Hacking Tool Value
SEA 6	Kali Linux 1

[Track All 6 Detections](#)

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 masques toutes les détections impliquant un service de numérisation externe.

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 based on findings found in your ExtraHop system. Confirm whether workstation20 is the victim of a malware or phishing attack.

OFFENDER

workstation20

192.168.165.168

Site: West

VICTIM

148.221.12.170

scanner.example.west

External Endpoint

SCANNER

Example Scanning Service Co.

Tune Detection

Create a rule to hide detections that match the following criteria. No detections are hidden from view and do not have notifications or alerts.

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.

Filter...

- Any External Scanning Service
- ✓ Example Scanning Service Co.

Cancel

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 ▾

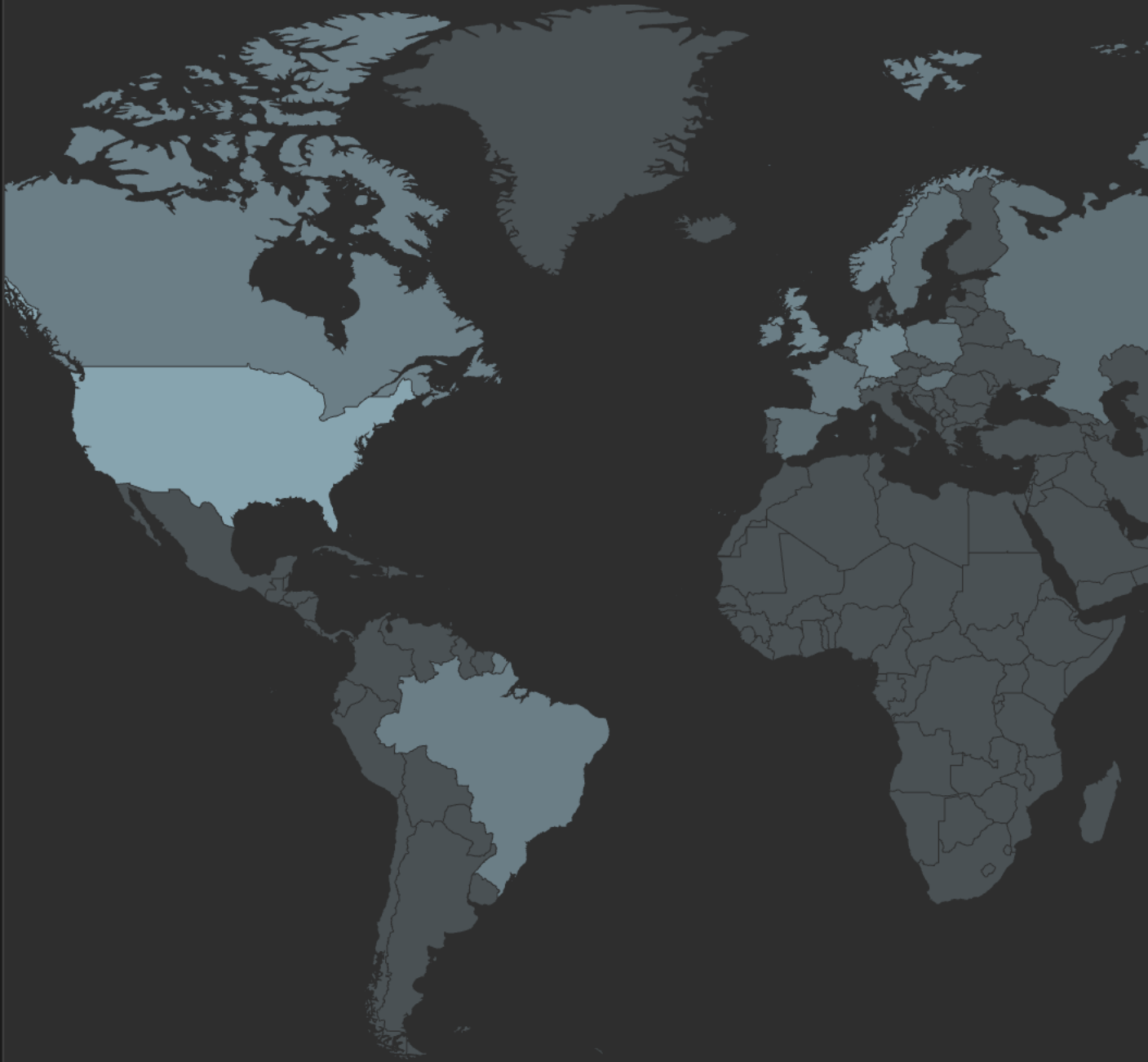
Overview / Perimeter

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.

The screenshot shows the ExtraHop interface with several security dashboards. On the left, there are sections for 'Informations sur les menaces' (listing threat briefings like 'Example Targeted Threat Briefing' and 'Shields Up briefing'), 'Recommandé pour le triage' (listing alerts like 'Unusual HTTP Plaintext Password'), and 'Types de détection' (showing counts for ATTAQUE: 16, DURCISSEMENT: 8, PERFORMANCE: 1). A central radar chart shows 'Détections par catégorie d'attaque' with values: RECON (508), EXPLOIT (519), LATERAL (0), and C&C (121). On the right, a 'Contrevenants fréquents' list shows IP addresses and device names like 'Cisco 65.155.239.28' and 'HSRP Router 004'. Below the dashboards is a navigation bar with links like 'Concepts', 'Comment faire', 'Procédures', 'Administration', 'Guides API', 'Déploiement', 'Déconnexion', and 'Lancer la Démo'. The main content area shows the 'Aperçu de la sécurité' page, which includes a description of the security overview, a 'Sélecteur de site' section, and a 'Version 9.4' dropdown menu with a 'Télécharger le PDF' button. A 'Ce sujet a-t-il été utile?' poll is also visible.

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.



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 connection

[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](#)

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

Recordstore Connection

June 28, 2023 09:18:30 UTC-08:00

The recordstore could not connect to the following sensors:

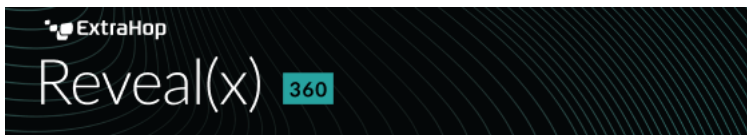
- sensor-sea-dc-01 (10.22.0.1)
- sensor-sea-dc-02 (10.22.96.9)

Review the sensor configuration or see the [Recordstore Troubleshooting](#) page.

Go to Reveal(x) 360 Sensor Configuration

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.



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.

[Go to User Access](#)