

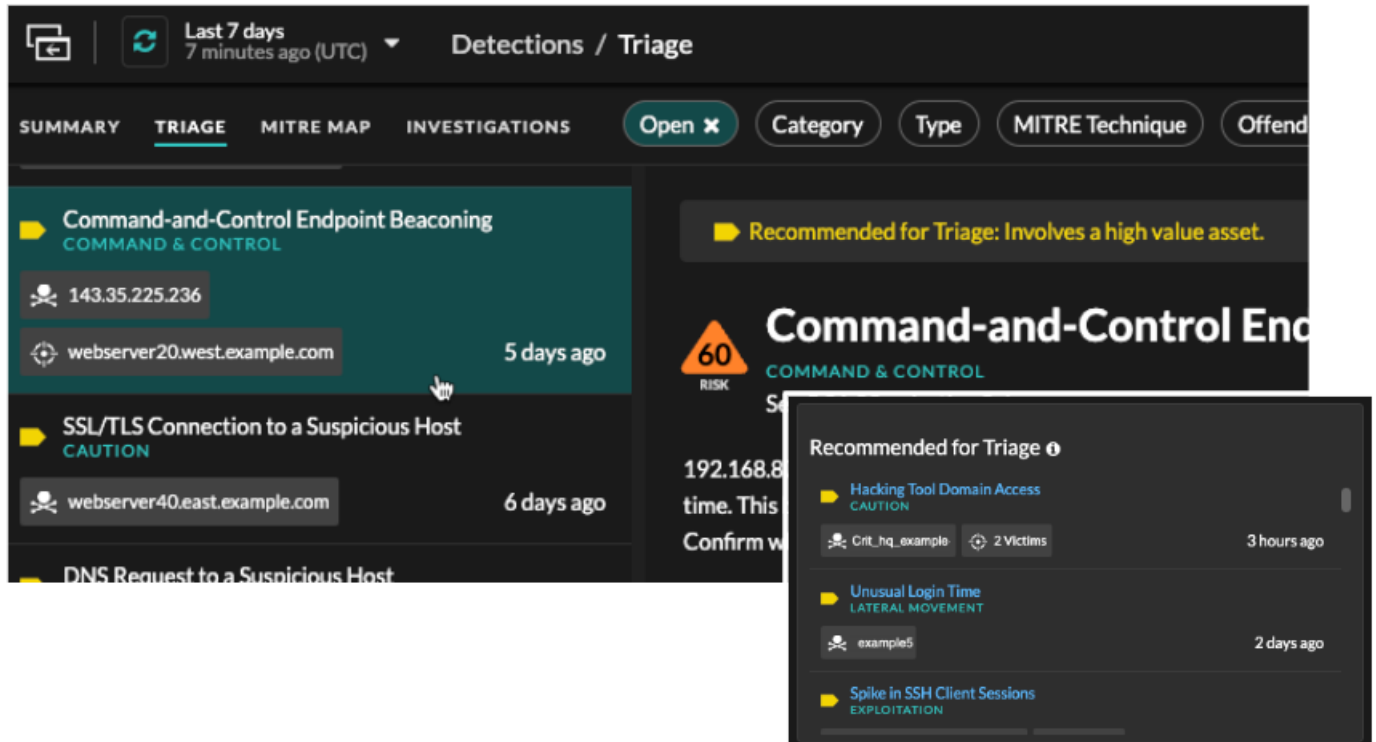
Was ist neu

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.

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

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

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](#)

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.

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. Matching detections are hidden from view and do not have notifications or trends.

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

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 ausgehenden Datenverkehr im Zusammenhang mit verbundenen internen Endpunkten anzuzeigen.

Was ist neu 3



Last 6 hours ▾

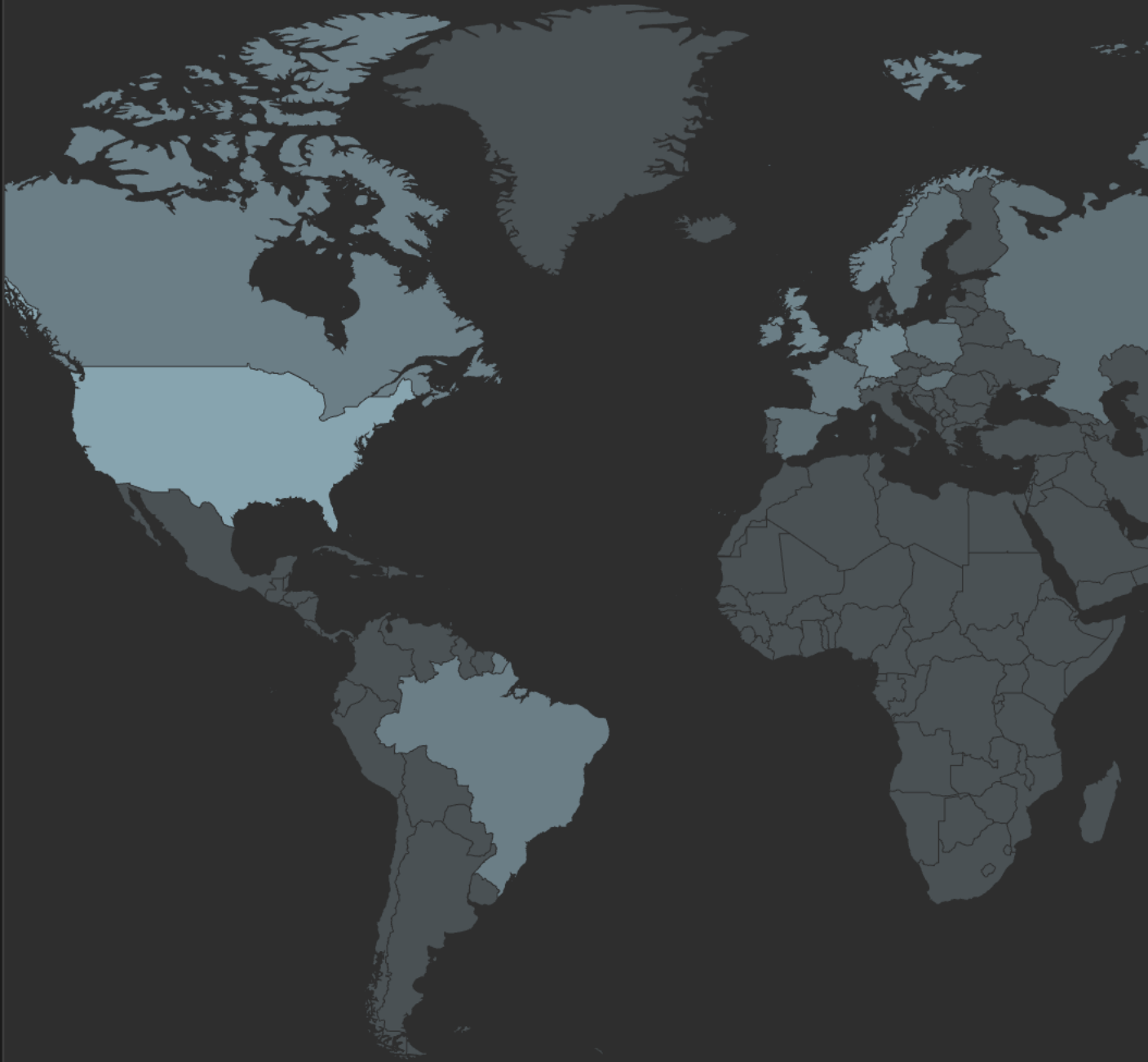
Overview / Perimeter

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.

The screenshot displays the ExtraHop security dashboard in French. The main content area includes:

- Informations sur les menaces:** Three threat intelligence items, including 'Example Targeted Threat Briefing' and 'State-Sponsored Activity (CISA Alert...)'. Each item has a risk level indicator (e.g., 'Risque Identifié').
- Types de détection:** Summary statistics showing 16 attacks, 8 hardening events, and 1 performance event.
- Détections par catégorie d'attaque:** A pie chart showing 508 Reconnaissance (RECON), 519 Exploits (EXPLOIT), 121 Credential Compromise (C&C), and 0 Lateral Movement (LATERAL) events.
- Contrevenants fréquents:** A list of IP addresses and device types associated with frequent offenses, such as Cisco routers and Adtran switches.
- Recommandé pour le triage:** A list of suspicious events, such as 'Unusual HTTP Plaintext Password' and 'DNS Request to a Suspicious Host'.

The right sidebar contains a navigation menu with links like 'Concepts', 'Comment faire', 'Procédures', 'Administration', 'Guides API', 'Déploiement', 'Déconnexion', and 'Lancer la Démo'. A language selector is set to 'Français', and there is a 'Télécharger le PDF' button for the current page.

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.



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](#)

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

Recordstore Connection

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

The recordstore could not connect to the following sensors:

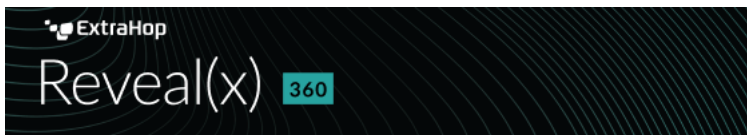
- sensor-sea-dc-01 (10.22.0.1)
- sensor-sea-dc-02 (10.22.96.9)

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

Go to Reveal(x) 360 Sensors

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.



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](#)