

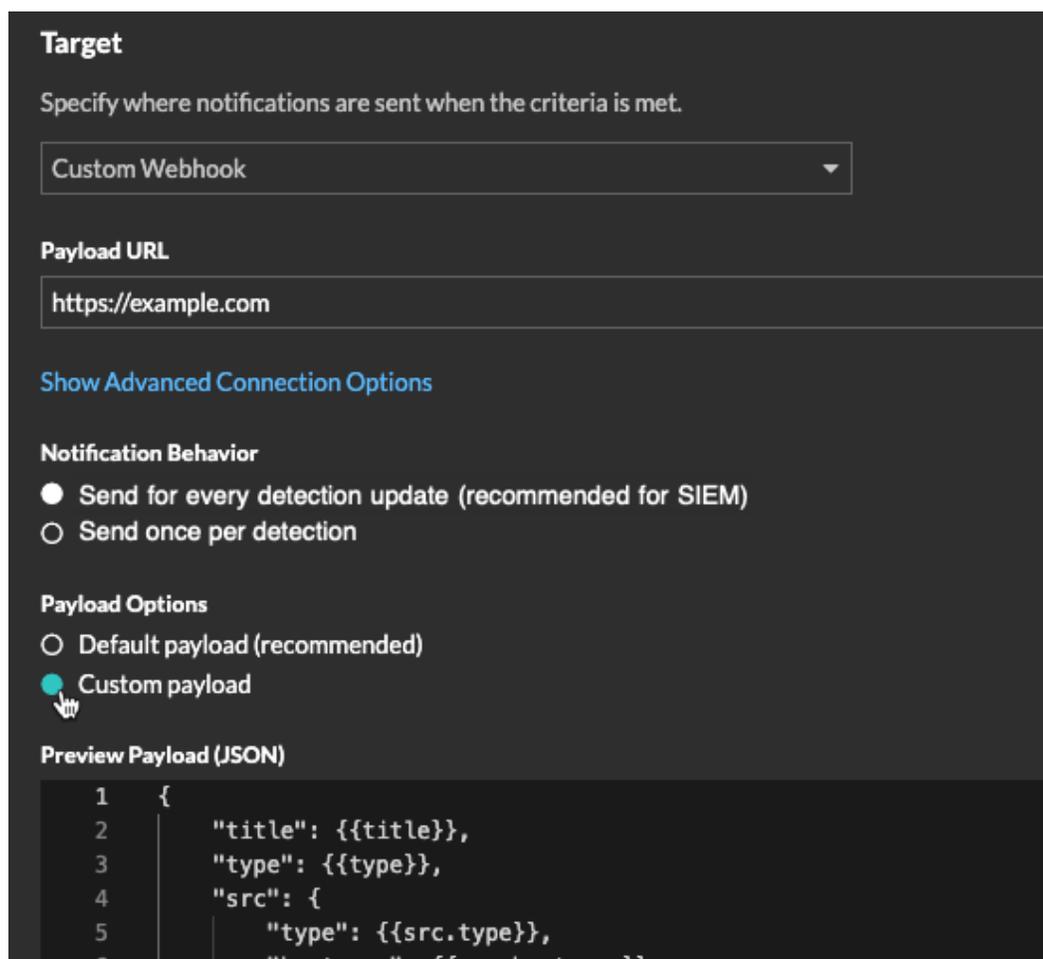
Quoi de neuf

Publié: 2024-10-26

Alors que [notes de version](#) pour un aperçu complet de nos mises à jour de versions, voici un aperçu des fonctionnalités les plus intéressantes d'ExtraHop 9.8.

Notifications de détection améliorées

Les détections et les notifications de détection ont été optimisées pour l'exportation de données de détection granulaires. Les utilisateurs peuvent désormais [configurer les règles de notification](#) pour envoyer une charge utile de webhook par défaut ou personnalisée pour chaque mise à jour de détection, ou envoyer une seule notification pour chaque détection.



The screenshot shows a configuration panel for notifications. It includes a 'Target' dropdown menu set to 'Custom Webhook', a 'Payload URL' field with 'https://example.com', and a 'Notification Behavior' section with two radio buttons: 'Send for every detection update (recommended for SIEM)' (selected) and 'Send once per detection'. Below that, the 'Payload Options' section has two radio buttons: 'Default payload (recommended)' and 'Custom payload' (selected). At the bottom, a 'Preview Payload (JSON)' section shows a code editor with a JSON structure: { "title": {{title}}, "type": {{type}}, "src": { "type": {{src.type}}, "hostname": {{src.hostname}} } }.

Rapport sur les opérations de sécurité

Vous pouvez désormais sélectionner le contenu à inclure dans [Rapport sur les opérations de sécurité](#) que vous générez à partir d'une page d'aperçu.

Generate Security Operations Report

Report Contents

- Attack Surface Visibility
- Threat Coverage
- Attack Detection
- Perimeter
- Security Hardening

Time Interval

- Last days
- Previous calendar week
- Previous calendar month

Sites

All Sites ▼

Report Options

- Include explanation text

Page Nouveaux fichiers

Le [Page des fichiers](#) affiche un tableau des fichiers hachés en fonction de filtres configurés et activés à partir des paramètres d'analyse des fichiers. Les détails des fichiers vous permettent d'étudier plus en détail le hachage des fichiers SHA-256 dans les appareils, les enregistrements, les détections et VirusTotal Lookup, un outil tiers.

The screenshot displays the ExtraHop RevealX 360 interface. The top navigation bar includes 'Overview', 'Dashboards', 'Detections', 'Alerts', 'Assets', 'Records', and 'Packets'. The 'Assets' tab is active, showing a search for files. The left sidebar lists navigation options: 'Devices', 'Device Groups', 'Files', 'Users', 'Applications', and 'Networks'. The main area shows a 'Find Files' search bar and a table of search results for 608 files. The table columns are: Filename, Media Type, SHA-256, Detections, Has Signature, File Size (Bytes), Locality, On Devices, and First Seen. A detailed view of a file is shown on the right, including its filename, media type, SHA-256 hash, detection status, and related information like other known filenames and detection details.

| Filename | Media Type | SHA-256 | Detections | Has Signature | File Size (Bytes) | Locality | On Devices | First Seen |
|------------------------------|---------------------|---------------|------------|---------------|-------------------|--------------------|------------|---------------------|
| product.xlsx | Document | 791c32a95f... | No | — | 12,000 | Outbound | 1 | 2024-04-23 11:05:29 |
| command.exe | Executable | cdc43c7e90... | Yes | Yes | 302 | Inbound, Internal | 3 | 2024-05-08 11:05:29 |
| log4j-web-2.20.0-sources.jar | Archive, Executable | 3a0d87b07a... | No | — | 14,000 | Internal | 2 | 2024-05-04 11:05:29 |
| presentation.pptx | Executable | f42d8f5095... | No | No | 8,000 | Inbound | 1 | 2024-05-04 11:05:29 |
| report.docx | Document | 6b26f19ef7... | Yes | — | 382 | Inbound | 1 | 2024-04-29 11:05:29 |
| company_policies.docx | Document | a7c9f9e107... | No | — | 3,000 | Internal | 975 | 2024-05-03 11:05:29 |
| proposal.pdf | Document | b19d3d181e... | No | — | 6,000 | Internal, Outbound | 1 | 2024-04-22 11:05:29 |
| schedule.xlsx | — | — | — | — | — | — | — | — |
| project_plan.docx | Document | — | — | — | — | — | — | — |
| expense_report.xlsx | Document | — | — | — | — | — | — | — |
| agenda.docx | Document | — | — | — | — | — | — | — |
| client_list.xlsx | Document | — | — | — | — | — | — | — |
| training_materials.pptx | Document | — | — | — | — | — | — | — |
| invoice.pdf | Document | — | — | — | — | — | — | — |
| policy_manual.docx | Document | — | — | — | — | — | — | — |
| timesheet.xlsx | Document | — | — | — | — | — | — | — |
| contract.pdf | Document | — | — | — | — | — | — | — |
| business_plan.docx | Document | — | — | — | — | — | — | — |
| marketing_plan.docx | Document | — | — | — | — | — | — | — |

Nouvelles intégrations avec RevealX 360

Intégrations SIEM de nouvelle génération

Intégrations ajoutées pour **SIEM de nouvelle génération CrowdStrike Falcon** et **Solution SIEM de sécurité d'entreprise Splunk** cet effet de levier **règles de notification** pour exporter les données de détection ExtraHop vers le SIEM cible.

EXTRAHOP | RevealX 360

Administration / Integrations

Integrations

Click any tile to learn more about integrations developed by ExtraHop and by our technology partners.

Configure

Configure

Integration Status

Status: ● Integration Enabled
 Proxy Sensor: ● prod-pdx-eda-6100v

[Send Test Event](#)
[Change Credentials](#)
[Delete Credentials](#)

Notification Rules

This integration is configured as the target for the following notification rules.

| Name | Event Type | Status | Author | |
|-------------------|-----------------------|--|-----------|----------------------|
| All System Alerts | Security Detection | ● Enabled | maeybluth | Edit |
| NOC | Performance Detection | ● Disabled | tobias | Edit |

[Add Notification Rule](#)

Intégrations entre LevelBlue, Axonius et Cisco XDR

Les nouvelles intégrations suivantes ont été ajoutées pour vous aider à étudier les données d'équipement et de détection et à y répondre :

- [Niveau bleu](#) propose une détection et une réponse gérées (MDR).
- [Axonius](#) est un outil de gestion des actifs de cybersécurité.
- [Cisco XDR](#) est une solution étendue de détection et de réponse basée sur le cloud.

EXTRAHOP | RevealX 360

Administration / Integrations

Integrations

Click any tile to learn more about integrations developed by ExtraHop and by our technology partners.

Configure

Configure

Configure

Pour les administrateurs

Contrôle d'accès aux paquets

Les administrateurs peuvent désormais accorder [privilèges](#) qui permettent aux utilisateurs de télécharger uniquement les en-têtes de paquets. Les administrateurs de RevealX 360 peuvent

également définir [politique mondiale](#) pour la taille des tranches de paquet, et [activer le contrôle d'accès aux sondes](#) pour accorder l'accès à des groupes d'utilisateurs spécifiques.

Edit Sensor Access Control

You can enable packet download restrictions by specifying a SAML attribute value that limits packet access to assigned sensors.

Options

- Enable packet download restrictions
- Limited access
On unassigned sensors, users with packet download privileges can download packet headers.
- No access
On unassigned sensors, users have no packet access regardless of privileges.

SAML Configuration

Specify an attribute name
SAML user group Manag

Packet and Session Key Access

- Packets and session keys
- Packets only
- Packet slices only
- Packet headers only
- No access

Packet Slice Download Control

Users with packet slices only privileges can download the first **64** bytes of a packet.

Save Changes

Mot de passe d'extraction de fichiers

Un mot de passe est nécessaire pour ouvrir les fichiers .zip extraits ou gravés à partir de paquets. Les administrateurs peuvent définir le mot de passe d'extraction des fichiers dans les paramètres d'administration de [RevealX Enterprise](#) ou [RevealX 360](#) et partager le mot de passe avec les utilisateurs autorisés.

File Extraction Password

Specify the password required for users to unzip files extracted and downloaded from a packet query.

Show Password Change Password

Décryptage pour plusieurs contrôleurs de domaine

Le système ExtraHop désormais [prend en charge la connexion de plusieurs contrôleurs de domaine](#) à une sonde pour déchiffrer le trafic du contrôleur de domaine. Vous pouvez configurer le déchiffrement sur une sonde individuelle sur RevealX Enterprise ou via une intégration sur RevealX 360.

ExtraHop
RevealX

Welcome, setup. Log Out Help

Admin > Capture > Domain Controller

Domain Controller

Configure connections between domain controllers and ExtraHop sensors that synchronize encryption keys, enabling you to decrypt, analyze, and detect threats on devices joined to the domain. Specify connection details and user credentials for each domain controller that you want to connect to this sensor.

Caution: Only highly-privileged users who are granted administrative access to the domain controller should have access to the ExtraHop system. [Learn more about configuring this setting securely.](#)

Status: ● Synced
Last Successful Sync: 2020/09/22 14:00

Host
englep1201500.ahresearch.com

Computer Name (sAMAccountName)
ITAdmin

Realm Name
EHRESEARCH

Username
ben

[Change User Credentials](#)

✓ The connection to the target was successful.

Host *

Computer Name (sAMAccountName) *

Realm Name *

Username *

Password *

[Add Domain Controller Connection](#)

Administration / Integrations / Splunk

Microsoft Protocol Decryption

Microsoft Protocol Decryption Integration

Integrate with a Microsoft Active Directory domain controller to enable decryption of Microsoft protocol traffic and improve detection of security attacks within your Microsoft Windows environment. ExtraHop RevealX 360 synchronizes encryption keys with Windows domain controllers to decrypt and analyze network traffic over protocols such as LDAP, RPC, SMB, and WSMan.

With this integration you can leverage RevealX 360 to detect threats to devices joined to the domain, gain deeper insights into detection details, and extend visibility to devices with encrypted Microsoft protocol traffic. The integration is restricted to read-only actions.

Integration Features

- ✓ Gain enhanced detection coverage and insights
- ✓ Gain enhanced device visibility into Microsoft protocol traffic
- ✓ View a decryption health dashboard

[Go to Integration Documentation](#)

Integration Status

Status: ● Up-to-date
Host: 10.15.6.19
Realm Name: TESTLOCAL
Sensor: server.sea.leh.com
Last Successful Sync: 2024/07/30 16:30
[Change Credentials](#) [Delete Credentials](#)

Connect to Another Domain Controller

Specify credentials to connect another Microsoft Active Directory domain controller to a RevealX 360 sensor.

Pour les développeurs d'API

API de déclenchement

Vous pouvez désormais stocker des métriques et accéder aux propriétés du trafic SOCKS et NMF avec le nouveau [SOCKS](#) et [NMF](#) cours.

API REST

A ajouté le `/appliances/sensortags` point de terminaison du [API REST RevealX 360](#), qui vous permet de visualiser et de gérer les étiquettes des sondes.