

# Was ist neu

Veröffentlicht: 2024-10-26

Während [Versionshinweise](#) geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.8.

## Verbesserte Erkennungsbenachrichtigungen

Erkennungen und Erkennungsbenachrichtigungen wurden für den Export granularer Erkennungsdaten optimiert. Benutzer können jetzt [Benachrichtigungsregeln konfigurieren](#) um eine standardmäßige oder benutzerdefinierte Webhook-Nutzlast für jedes Erkennungsupdate zu senden oder nur eine Benachrichtigung für jede Erkennung zu senden.

### Target

Specify where notifications are sent when the criteria is met.

Custom Webhook

### Payload URL

https://example.com

[Show Advanced Connection Options](#)

### Notification Behavior

Send for every detection update (recommended for SIEM)

Send once per detection

### Payload Options

Default payload (recommended)

Custom payload

### Preview Payload (JSON)

```
1  {
2    "title": {{title}},
3    "type": {{type}},
4    "src": {
5      "type": {{src.type}},
6      "hostname": {{src.hostname}}
```

## Bericht über Sicherheitsoperationen

Sie können jetzt den Inhalt auswählen, der in eine aufgenommen werden soll [Bericht über Sicherheitsoperationen](#) die Sie von einer Übersichtsseite aus generieren.

## 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

### Seite „Neue Dateien“

Das [Seite „Dateien“](#) zeigt eine Tabelle mit Dateien an, die gemäß Filtern gehasht wurden, die in den Dateianalyse-Einstellungen konfiguriert und aktiviert wurden. Mithilfe von Dateidetails können Sie den SHA-256-Datei-Hash in Geräten, Datensätzen, Erkennungen und VirusTotal Lookup, einem Drittanbieter-Tool, weiter untersuchen.

The screenshot displays the ExtraHop Reveal(x) 360 interface. The top navigation bar includes 'Overview', 'Dashboards', 'Detections', 'Alerts', 'Assets', 'Records', and 'Packets'. The 'Assets' tab is active, showing a 'Find Files' search interface. The search results are displayed in a table with columns: Filename, Media Type, SHA-256, Detections, Has Signature, File Size (Bytes), Locality, On Devices, and First Seen.

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	—	—	—	—	—	—	—

The interface also shows a 'Find Files' search bar with filters for 'File Size > 1,000,000 Bytes' and 'Locality = Outbound'. The search results are displayed in a table with columns: Filename, Media Type, SHA-256, Detections, Has Signature, File Size (Bytes), Loc, and Details.

Filename	Media Type	SHA-256	Detections	Has Signature	File Size (Bytes)	Loc	Details
productquery.exe	Executable	791c32a95f...	Yes	No	3,000,000	Out	<p>Filename: productquery.exe</p> <p>Other Known Filenames: productquery2.exe, productquery1.exe</p> <p>Media Type: Executable</p> <p>SHA-256: 791c32a95f4017464214960e49e716656f666ff135ac2a6ba607236d3346ex</p> <p>Detections: Yes</p> <p>Has Signature: No</p> <p>Locality: Outbound</p> <p>File Size: 3MB</p> <p>On Devices: 1</p> <p>First Seen: 2024-04-23 11:05:29</p> <p>Go To</p> <ul style="list-style-type: none"> <li>VirusTotal Lookup</li> <li>Related Devices</li> <li>Related Records</li> <li>Related Detections</li> </ul>
command.exe	Executable	cdc43c7e90...	No	Yes	2,000	Out	
budget.xlsx	Document	3a0d87b07a...	No	—	58,000	Inb	
presentation.pptx	Executable	f42d8f5095...	No	No	68,000	Inb	
report.docx	Document	6b26f19ef7...	No	—	208,000	Inb	

## Neue RevealX 360-Integrationen

### SIEM-Integrationen der nächsten Generation

Integrationen hinzugefügt für [CrowdStrike Falcon SIEM der nächsten Generation](#) und [Splunk SIEM für Unternehmenssicherheit](#) diese Hebelwirkung [Regeln für Benachrichtigungen](#) um ExtraHop-Erkennungsdaten in das Ziel-SIEM zu exportieren.

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	<span style="color: green;">●</span> Enabled	maebybluth	<a href="#">Edit</a>
NOC	Performance Detection	<span style="color: gray;">●</span> Disabled	tobias	<a href="#">Edit</a>

[Add Notification Rule](#)

### Integrationen von LevelBlue, Axonius und Cisco XDR

Die folgenden neuen Integrationen wurden hinzugefügt, um Ihnen zu helfen, Gerät- und Erkennungsdaten zu untersuchen und darauf zu reagieren:

- **Level Blau** [🔗](#) bietet Managed Erkennung and Response (MDR).
- **Axonius** [🔗](#) ist ein Tool zur Verwaltung Asset Cybersicherheitsressourcen.
- **Cisco XDR** [🔗](#) ist eine Cloud-basierte erweiterte Erkennung- und Reaktionslösung.

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

### Für Administratoren

#### Paketzugriffskontrolle

Administratoren können jetzt gewähren **Privilegien** [🔗](#) die es Benutzern ermöglichen, nur Paket-Header herunterzuladen. RevealX 360-Administratoren können auch eine einrichten **globale Politik** [🔗](#)

für Paketsegmentgröße und [Sensorzugriffskontrolle aktivieren](#) um bestimmten Benutzergruppen Zugriff zu gewähren.

**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.

**Packet and Session Key Access**

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

**SAML Configuration**

Specify an attribute name  
SAML user group Manager

**Packet Slice Download Control**

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

Save Changes

### Passwort für die Dateixtraktion

Zum Öffnen von .zip-Dateien, die aus Paketen extrahiert oder geschnitten wurden, ist ein Passwort erforderlich. Administratoren können das Passwort für die Dateixtraktion in den Administrationseinstellungen auf festlegen [RevealX Enterprise](#) oder [RevealX 360](#) und teilen Sie das Passwort mit zugelassenen Benutzern.

**File Extraction Password**

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

\*\*\*\*\*

Show Password Change Password

### Entschlüsselung für mehrere Domänencontroller

Das ExtraHop-System jetzt [unterstützt die Verbindung mehrerer Domänencontroller](#) zu einem Sensor, um den Domänencontroller-Verkehr zu entschlüsseln. Sie können die Entschlüsselung auf einem einzelnen Sensor auf RevealX Enterprise oder über eine Integration auf RevealX 360 konfigurieren.

The image shows two screenshots from the ExtraHop web interface. The left screenshot is the 'Domain Controller' configuration page, which includes a search bar, navigation links, and a status section indicating a successful sync on 2020/09/23 14:00. Below this are input fields for Host, Computer Name, Realm Name, Username, and Password, along with 'Test Connection', 'Remove Connection', and 'Save' buttons. A success message at the bottom states 'The connection to the target was successful.' The right screenshot shows the 'Microsoft Protocol Decryption' integration status page, featuring a status indicator (Up-to-date), host information (10.15.6.19), realm name (TESTLOCAL), and sensor details (server.sea.leh.com). It also displays the last successful sync time (2024/07/30 16:30) and provides options to change or delete credentials. A section titled 'Connect to Another Domain Controller' includes an 'Add Credentials' button and a note to specify credentials for another Microsoft Active Directory domain controller.

## Für API-Entwickler

### API auslösen

Sie können jetzt Metriken speichern und auf Eigenschaften für SOCKS- und NMF-Verkehr zugreifen mit neuen **SOCKS** [🔗](#) und **NMF** [🔗](#) Klassen.

### REST-API

Das wurde hinzugefügt `/appliances/sensortags` Endpunkt zum **RevealX 360 REST-API** [🔗](#), mit dem Sie Sensor-Tags anzeigen und verwalten können.