

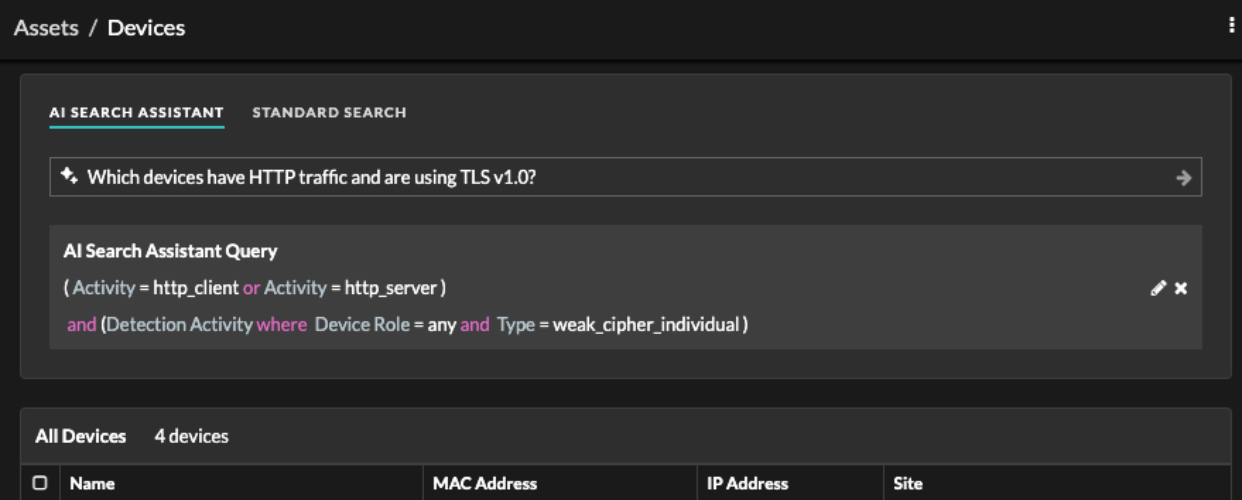
Was ist neu

Veröffentlicht: 2024-04-10

Während [Versionshinweise](#) geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.6.

KI-Suchassistent

[Häufig gestellte Fragen zum AI-Suchassistenten](#) ermöglicht es Ihnen, Suchvorgänge von der Assets-Seite aus zu starten, indem Sie eine Frage zu Geräten eingeben, die auf dem ExtraHop-System beobachtet wurden. Diese Frage oder Aufforderung wird Filterkriterien zugeordnet und gibt Suchergebnisse zurück. Administratoren von Reveal (x) 360 und Reveal (x) Enterprise müssen sich für diese Funktion anmelden, die standardmäßig deaktiviert ist.



Assets / Devices

AI SEARCH ASSISTANT STANDARD SEARCH

Which devices have HTTP traffic and are using TLS v1.0?

AI Search Assistant Query

(Activity = http_client or Activity = http_server)

and (Detection Activity where Device Role = any and Type = weak_cipher_individual)

All Devices 4 devices

<input type="checkbox"/>	Name	MAC Address	IP Address	Site
--------------------------	------	-------------	------------	------

Geplante Berichte für Führungskräfte

Executive Reports enthalten eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. Von einer Konsole aus können Sie jetzt [einen geplanten Executive Report erstellen](#) das beinhaltet Daten aus einem benutzerdefinierten Zeitintervall, das als PDF per E-Mail an bestimmte Empfänger gesendet wird

Create Scheduled Report

Properties

Report Name
Weekly Executive Report

Description
Report for the previous week - send Monday mornings

Owner
shellie

Report Type
 Dashboard
 Executive

Report Contents
Executive Report

Sites
All Sites

Schedule

Time Interval
 Last 24 days
 Previous calendar week
 Previous calendar month

Report Frequency
 Weekly Monthly

At: 09:00 Canada/Newfoundland

On: M T W Th F S Su

[Add Schedule](#)

MARCH 24 – 30, 2024

ExtraHop
Reveal(x) Enterprise

EXECUTIVE REPORT

This report is for the following sites:
polaris-ids.sns.Extrahop.com, Polaris 2, Polaris 3

MARCH 24 – 30, 2024 EXECUTIVE REPORT

SUMMARY

This report contains a summary of the top detections and potential risks to your network as identified by your ExtraHop system for the

Attack Detections	3,039	Highest Risk Score	88
Assets with Detections	1,360	Internal Endpoints Accepting Inbound Connections	393

210% ↑ since last week

85 → 84 since last week

Suche nach Geräten anhand der Erkennungsaktivität

Du kannst jetzt [Suche nach Geräten anhand ihrer zugehörigen Erkennungsaktivität](#). Fügen Sie Ihrem Suchfilter die Option Kriterien für Erkennungsaktivitäten hinzu und verfeinern Sie dann Ihre Suche weiter mit Kriterien wie Erkennungskategorien, Risikobewertungen und MITRE-Techniken.

The screenshot shows the ExtraHop 'Assets / Devices' page. The search results show 418 devices. An 'Advanced Filter' dialog is open, showing the following criteria:

- MATCH: Software = CrowdStrike Falcon
- AND: Detection Activity As Participant
- WHERE: Category = Command & Control
- AND: Risk Score > 75
- AND: Status = In Progress

Intelligente Ermittlungen

Der ExtraHop Machine Learning Service jetzt **empfiehlt Untersuchungen** wenn Netzwerkaktivitäten mit einer Reihe bekannter Angriffstechniken übereinstimmen, sodass Ihre Sicherheitsteams böswartiges Verhalten schnell einschätzen und darauf reagieren können.

The screenshot shows the 'C&C with Exfiltration' investigation page. It includes a 'Recommended Investigation' section with a description: 'A device on your network was the victim in a command-and-control (C&C) detection, then became the offender in an exfiltration detection.' The page is divided into three main sections:

- Attack Progression:** Command & Control (1), Reconnaissance (0), Exploitation (0), Lateral Movement (0), Actions on C...
- Detections:** 2 detections linked in this investigation.
 - Apr 2 10:03 • 3 hours ago: Meterpreter C&C Session (COMMAND & CONTROL) with IP 125.67.28.39 and host webserv.east.example.
 - Apr 2 10:03 • 3 hours ago: Data Exfiltration (ACTIONS ON OBJECTIVE, EXFILTRATION) with host webserv.east.example and IP 151.92.230.221.
- Participants:** 2 participants linked in this investigation.
 - External Endpoints:** 62.144.181.162 (test.example.com).
 - Recurring Participants:** webserv.east.example (192.168.16.42, Site: East).
- Status and Response Actions:** Last edited by sean on Apr 02 12:34. Status: IN PROGRESS. Assessment: Undecided. Assignee: garyp.
- Notes:** Reviewed with team. Gary to take lead here. - Sean

TAXII Feeds

Bedrohungsinformationen können jetzt über einen Trusted Automated Exchange of Intelligence Information (TAXII) -Feed an Ihr ExtraHop-System übertragen werden. **Einen TAXII-Feed hinzufügen** für einen konsistenten Strom aktueller Bedrohungsindikatoren, die Sie aktivieren können, um verdächtige Endpunkte hervorzuheben und Erkennungen zu generieren.

TAXII Feed
Add a TAXII feed to provide an up-to-date stream of threat indicators.

Name: ExampleFeed 1
TAXII Server Discovery URL: https://example.taxii.feed.com/
Collections: Brute Force List, VulnFeed, Cyberscout Analysis
Maximum Lookback: 15 days
Polling Frequency: 6 hours
Indicators: 10,136
[Edit](#) [Remove](#)

Threat Intelligence

SUSPICIOUS Threat Intelligence Indicator for suspicious-example.com
Type: SUNBURST Backdoor

59 Offenders

27.226.40.82 **SUSPICIOUS**
206.87.153.126
143.58.100.52
177.82.221.79 **SUSPICIOUS**
125.80.192.93

OFFENDER

IP 34.223.124.45
suspicious-example.com
MALICIOUS

TAXII Collections

TAXII Feed	Collection	Imported Indicators	Match Result	Status	Last Polled
ExampleFeed 1	Brute Force List	4,326	Detection Enrichment and Creation	Up-to-date	2024-03-22 12:41:58
ExampleFeed 1	Cyberscout Analysis	2,902	Detection Enrichment	Up-to-date	2024-03-22 12:41:01
ExampleFeed 1	VulnFeed	1,093	Detection Enrichment	Failed to update	2024-03-22 12:45:34

Pakete

Auf dem [Pakete](#) Auf dieser Seite können Sie im Fenster Neue Paketabfrage eine verfeinerte Abfrage erstellen, die nur die Ergebnisse zurückgibt, die Sie benötigen.

New Packet Query All Sensors ▾

Select a field to search on: **IP Address** | MAC Address | BPF | Port | EtherType | VLAN ID | IP Protocol

=

[View Packets](#)

Select a sensor

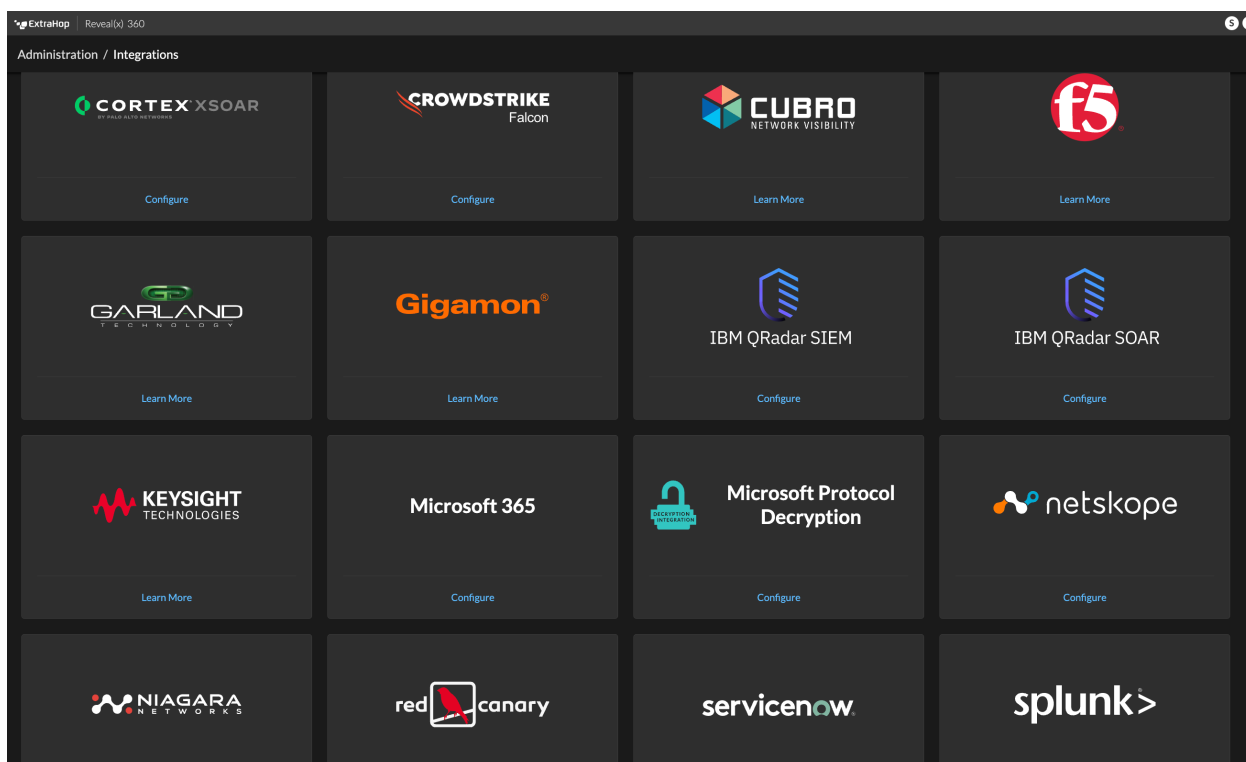
Type any string such as an IP address, MAC address, or port number to search on

Click to start a packet query

Neue Integrationen

ExtraHop Reveal (x) 360-Integrationen Dazu gehören Anbieter, die gemeinsame Produktlösungen anbieten, und Apps von Drittanbietern, die in die ExtraHop REST-API integriert sind. Die folgenden Produkte und Anbieter wurden der Integrationsseite hinzugefügt:

- Cubro
- F5 Networks LTM
- Girlande PacketMax
- Gigamon
- IBM Security QRadar SOAR
- Keysight
- Niagara-Netzwerke
- Roter Kanarienvogel MDR
- ServiceNow Service Graph-Konnektor
- Zinken



Für Administratoren

Administratoren können sich dafür entscheiden, Netzwerkdaten anhand einer **erweiterte Bibliothek mit Bedrohungsinformationen** [🔗](#), einschließlich einer zusätzlichen Sammlung von CrowdStrike-Indikatoren, gutartigen Endpunkten und anderen Informationen zum Netzwerkverkehr, die das Rauschen reduzieren und die Erkennung verbessern können.

Für API-Entwickler

Sie können jetzt Untersuchungen anzeigen, aktualisieren und erstellen über das **REST-API für Untersuchungen** [🔗](#) Ressource.