

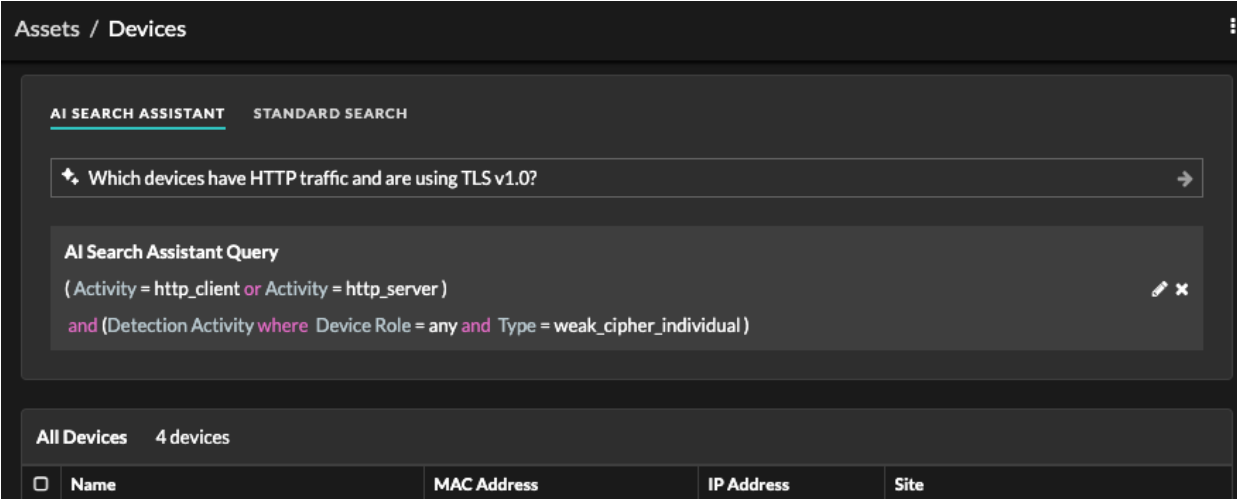
# What's New

Published: 2024-04-09

While [release notes](#) provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.6.

## AI Search Assistant

[AI Search Assistant FAQ](#) enables you to initiate searches from the Assets page by typing a question about devices observed on the ExtraHop system. That question, or prompt, is mapped to filter criteria and returns search results. Reveal(x) 360 and Reveal(x) Enterprise administrators must opt-in to this feature, which is disabled by default.



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
--------------------------	------	-------------	------------	------

## Scheduled Executive Reports

Executive reports contain a summary of the top detections and risks to your network. From a console, you can now [create a scheduled executive report](#) that includes data from a custom time interval that is emailed as a PDF to specified recipients

### 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

210% ↑ since last week

## Search for Devices by Detection Activity

You can now [search for devices by their associated detection activity](#). Add the Detection Activity criteria option to your search filter, and then refine your search further with criteria such as detection categories, risk scores, and MITRE techniques.

The screenshot shows the ExtraHop interface with the 'Assets / Devices' page. An 'Advanced Filter' dialog is open, showing the following conditions:

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

The background interface shows search results for 418 devices, with columns for Name and MAC Address.

## Smart Investigations

The ExtraHop Machine Learning Service now **recommends investigations** when network activity matches a series of known attack techniques, enabling your security teams to quickly assess and respond to malicious behavior.

The screenshot displays the 'C&C with Exfiltration' investigation page. Key details include:

- Recommended Investigation:** A device on your network was the victim in a command-and-control (C&C) detection, then became the offender in an exfiltration detection.
- Attack Progression:** Command & Control (1), Reconnaissance (0), Exploitation (0), Lateral Movement (0), Actions on Objective (0).
- 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 webservers.east.example.
  - Apr 2 10:03 • 3 hours ago: Data Exfiltration (ACTIONS ON OBJECTIVE, EXFILTRATION) with host webservers.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: webservers.east.example (192.168.16.42, Site: East).
- Status and Response Actions:** Status is IN PROGRESS. Assignee is garyp.
- Notes:** Reviewed with team. Gary to take lead here. - Sean

## TAXII Feeds

Threat intelligence can now be delivered to your ExtraHop system through a Trusted Automated Exchange of Intelligence Information (TAXII) feed. **Add a TAXII feed** for a consistent stream of up-to-date threat indicators that you can enable to highlight suspicious endpoints and generate detections.

**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  
Extraction: ...

**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

## Packets

On the [Packets](#) page, the New Packet Query window enables you to create a refined query that returns only the results you need.

**New Packet Query**

All Sensors ▾

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

= ▾

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

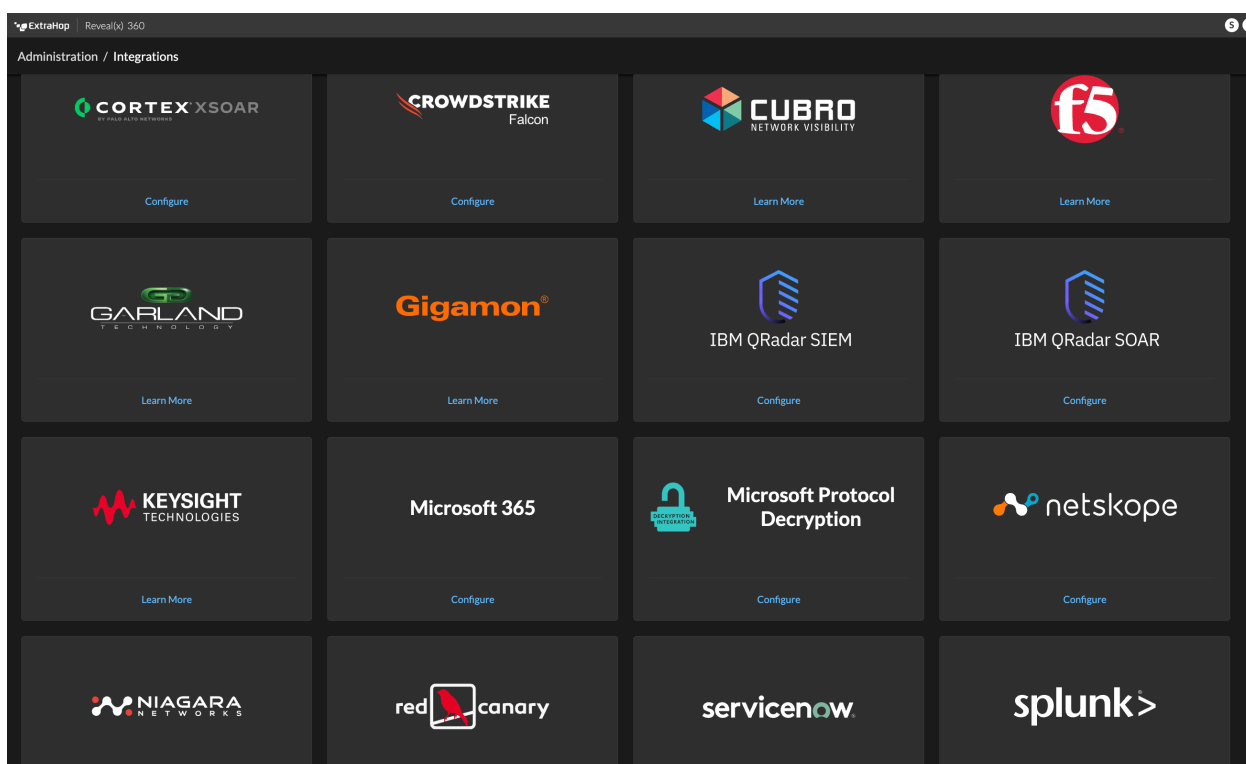
[View Packets](#)

Click to start a packet query

## New Integrations

[ExtraHop Reveal\(x\) 360 integrations](#) include vendors that offer joint product solutions and third-party apps that integrate with the ExtraHop REST API. The following products and vendors have been added to the Integrations page:

- Cubro
- F5 Networks LTM
- Garland PacketMAX
- Gigamon
- IBM Security QRadar SOAR
- Keysight
- Niagara Networks
- Red Canary MDR
- ServiceNow Service Graph Connector
- Tines



### For Administrators

Administrators can opt-in to have network data reviewed against an [expanded library of threat intelligence](#), including an additional collection of CrowdStrike indicators, benign endpoints, and other network traffic information that can reduce noise and improve detections.

### For API Developers

You can now view, update, and create investigations through the [Investigations REST API](#) resource.