

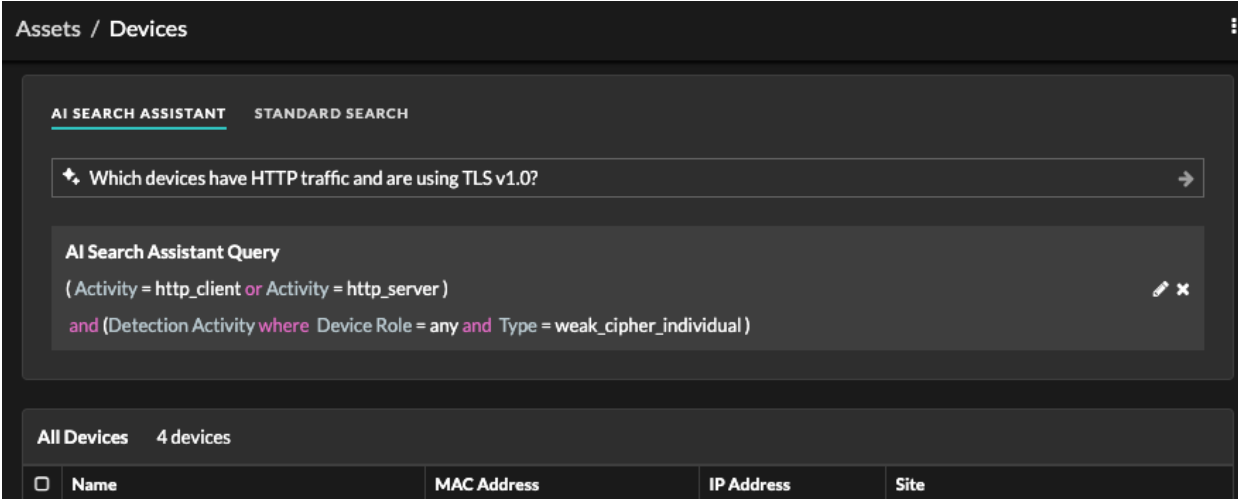
Quoi de neuf

Publié: 2024-04-10

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 9.6.

Assistant de recherche IA

[FAQ sur l'assistant de recherche AI](#) vous permet de lancer des recherches à partir de la page Ressources en saisissant une question sur les appareils observés sur le système ExtraHop. Cette question, ou invite, est associée à des critères de filtrage et renvoie des résultats de recherche. Les administrateurs de Reveal (x) 360 et Reveal (x) Enterprise doivent activer cette fonctionnalité, qui est désactivée par défaut.



The screenshot shows the 'Assets / Devices' section of the ExtraHop interface. It features two tabs: 'AI SEARCH ASSISTANT' (selected) and 'STANDARD SEARCH'. A search bar contains the query: 'Which devices have HTTP traffic and are using TLS v1.0?'. Below the search bar, the 'AI Search Assistant Query' is displayed as a logical expression: '(Activity = http_client or Activity = http_server) and (Detection Activity where Device Role = any and Type = weak_cipher_individual)'. At the bottom, a summary indicates 'All Devices 4 devices' and a table with columns for Name, MAC Address, IP Address, and Site.

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

Rapports exécutifs prévus

Les rapports exécutifs contiennent un résumé des principales détections et des principaux risques auxquels votre réseau est exposé. Depuis une console, vous pouvez désormais [créer un rapport exécutif planifié](#) qui inclut des données provenant d'un intervalle de temps personnalisé qui sont envoyées par e-mail au format PDF à des destinataires spécifiques

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
	210% ↑ since last week		85 → 84 since last week
Assets with Detections	1,360	Internal Endpoints Accepting Inbound Connections	393

Rechercher des appareils par activité de détection

Tu peux maintenant [rechercher des appareils en fonction de leur activité de détection associée](#). Ajoutez l'option Critères d'activité de détection à votre filtre de recherche, puis affinez votre recherche à l'aide de critères tels que les catégories de détection, les scores de risque et les techniques MITRE.

The screenshot shows the ExtraHop 'Assets / Devices' page. A search filter 'Software = CrowdStrike Falcon' is applied, resulting in 418 devices. An 'Advanced Filter' dialog is open, showing the following configuration:

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

Enquêtes intelligentes

Le service d'apprentissage automatique ExtraHop est désormais disponible [recommande des enquêtes](#) lorsque l'activité du réseau correspond à une série de techniques d'attaque connues, ce qui permet à vos équipes de sécurité d'évaluer rapidement les comportements malveillants et d'y répondre.

The screenshot shows the 'C&C with Exfiltration' investigation page. It features a 'Recommended Investigation' section with a summary of the attack progression:

- Command & Control: 1
- Reconnaissance: 0
- Exploitation: 0
- Lateral Movement: 0
- Actions on Objective: 0

The 'Detections' section shows two linked detections:

- Meterpreter C&C Session** (Command & Control): Apr 2 10:03 • 3 hours ago. IP: 125.67.28.39, Target: webservers.east.example.
- Data Exfiltration** (Actions on Objective, Exfiltration): Apr 2 10:03 • 3 hours ago. Target: webservers.east.example, IP: 151.92.230.221.

The 'Participants' section shows two participants:

- External Endpoints:** 62.144.181.162 (test.example.com).
- Recurring Participants:** webservers.east.example (192.168.16.42, Site: East).

The 'Status and Response Actions' section shows the status as 'IN PROGRESS' and the assignee as 'garyp'.

Flux TAXII

Les renseignements sur les menaces peuvent désormais être transmis à votre système ExtraHop via un flux TAXII (Trusted Automated Exchange of Intelligence Information). [Ajouter un flux TAXII](#) pour un flux constant d'indicateurs de menace à jour que vous pouvez activer pour mettre en évidence les terminaux suspects et générer des détections.

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

Paquets

Sur le [Paquets](#) page, la fenêtre New Packet Query vous permet de créer une requête affinée qui renvoie uniquement les résultats dont vous avez besoin.

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

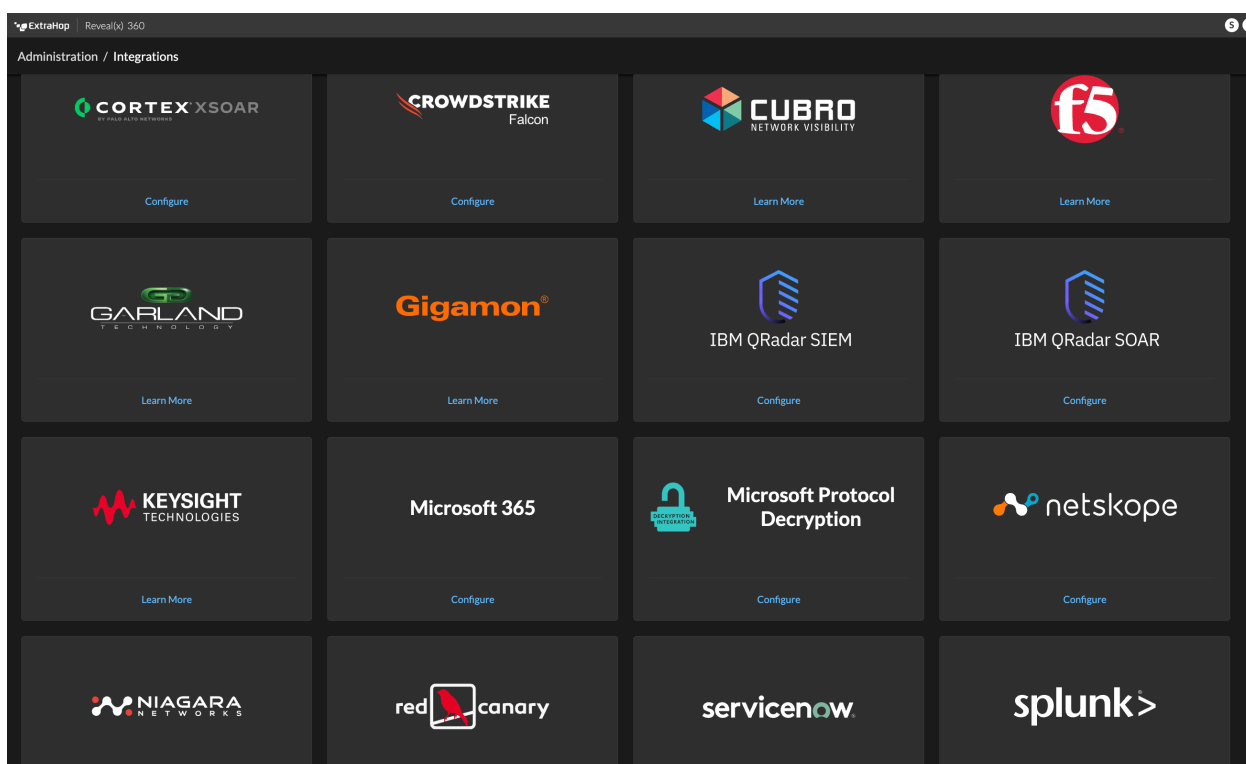
Type any string such as an IP address, MAC address, or port number to search on

Click to start a packet query

Nouvelles intégrations

Intégrations ExtraHop Reveal (x) 360 inclure des fournisseurs qui proposent des solutions de produits communes et des applications tierces qui s'intègrent à l'API REST ExtraHop. Les produits et fournisseurs suivants ont été ajoutés à la page Intégrations :

- Cubro
- F5 Networks LTM
- Guirlande PacketMax
- Gigamon
- IBM Security QRadar SOAR
- Keysight
- Réseaux Niagara
- Red Canary MDR
- Connecteur ServiceNow Service Graph
- Dents



Pour les administrateurs

Les administrateurs peuvent choisir de faire examiner les données du réseau par rapport à [bibliothèque élargie de renseignements sur les menaces](#), y compris une collection supplémentaire d'indicateurs CrowdStrike, de points de terminaison inoffensifs et d'autres informations sur le trafic réseau susceptibles de réduire le bruit et d'améliorer les détections.

Pour les développeurs d'API

Vous pouvez désormais consulter, mettre à jour et créer des enquêtes via [API REST Investigations](#) ressource.