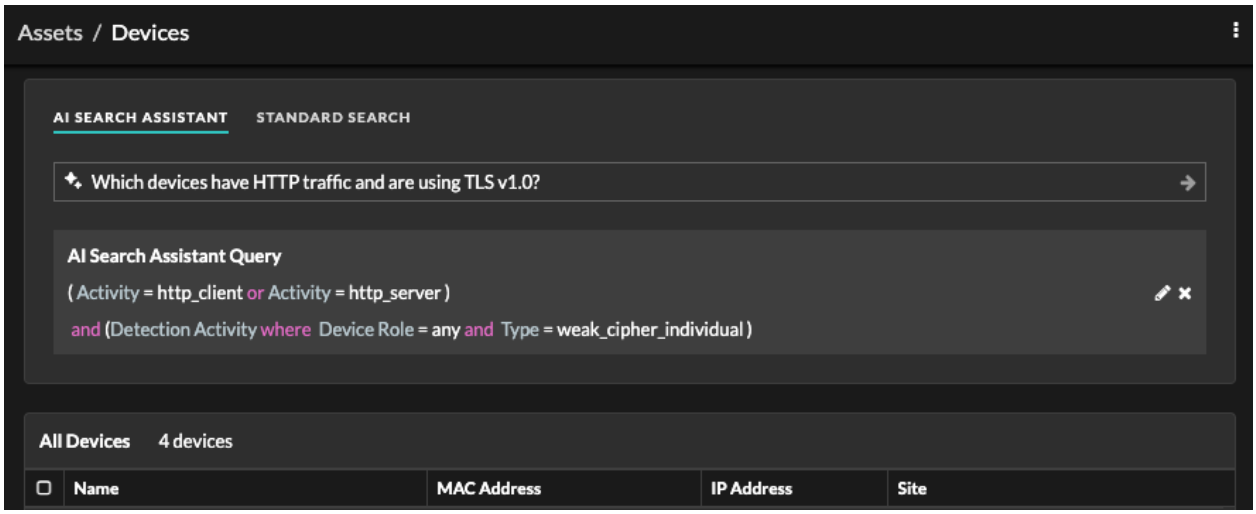
What's New

Published: 2025-01-15

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

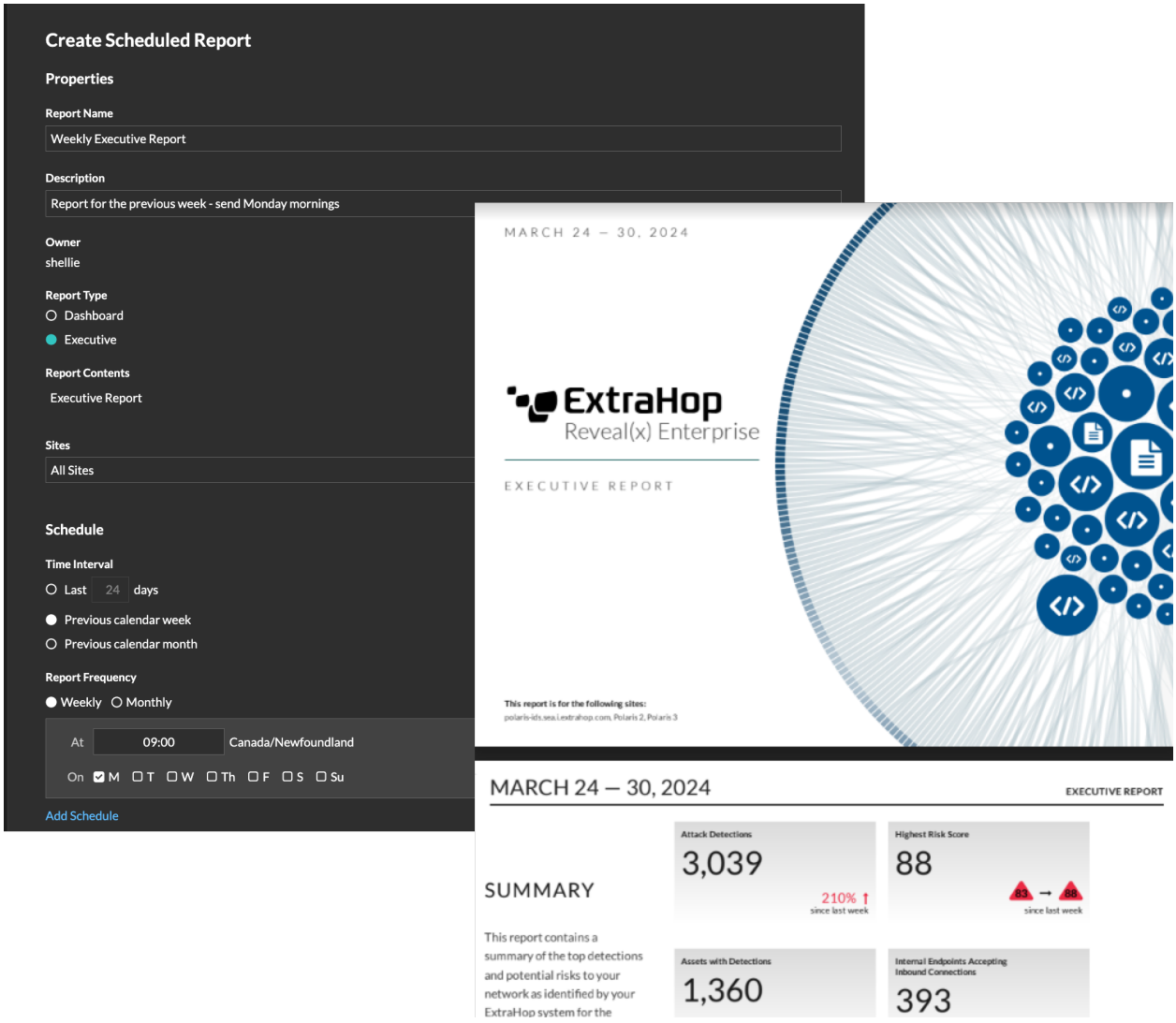
AI Search Assistant

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.



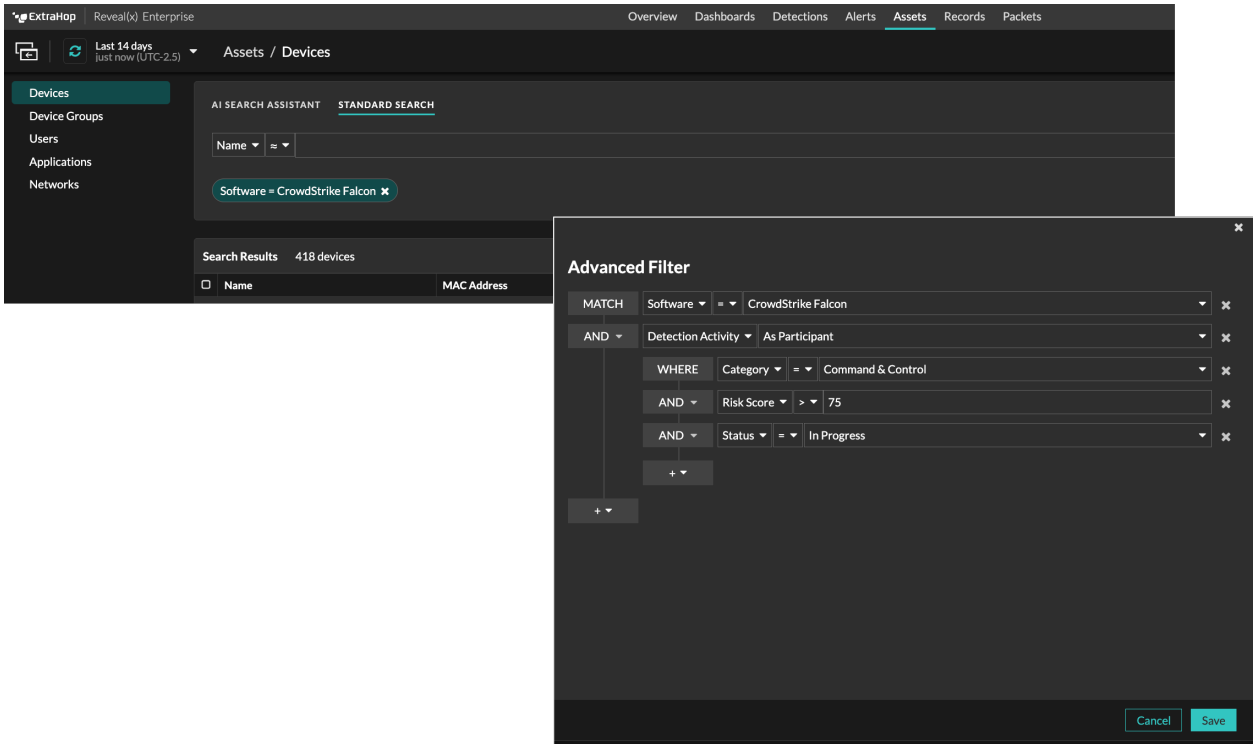
Scheduled Executive Reports

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



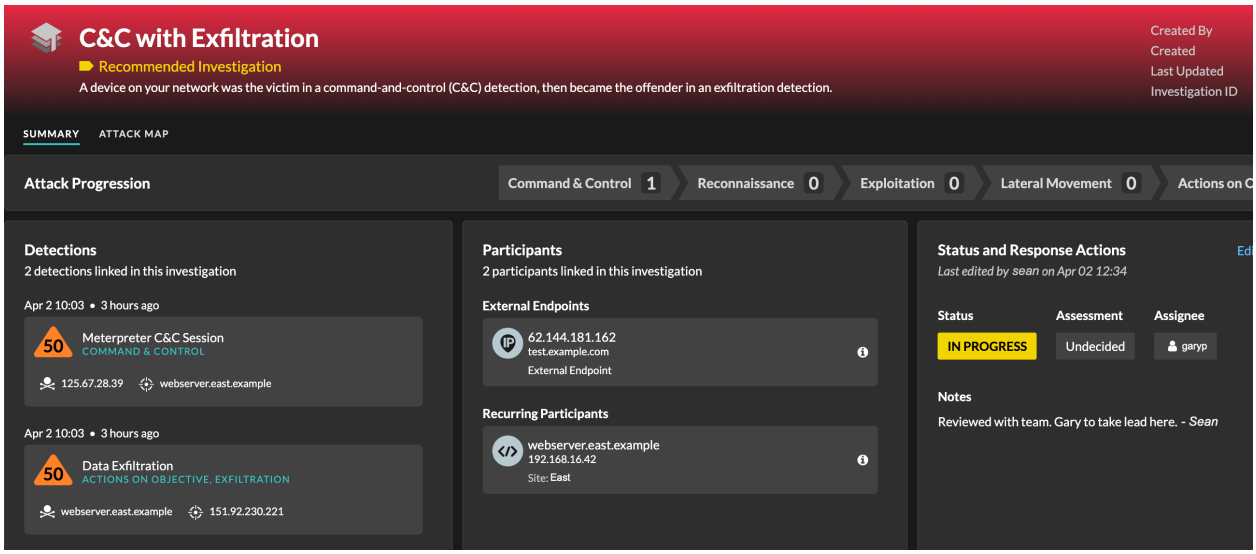
Search for Devices by Detection Activity

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.



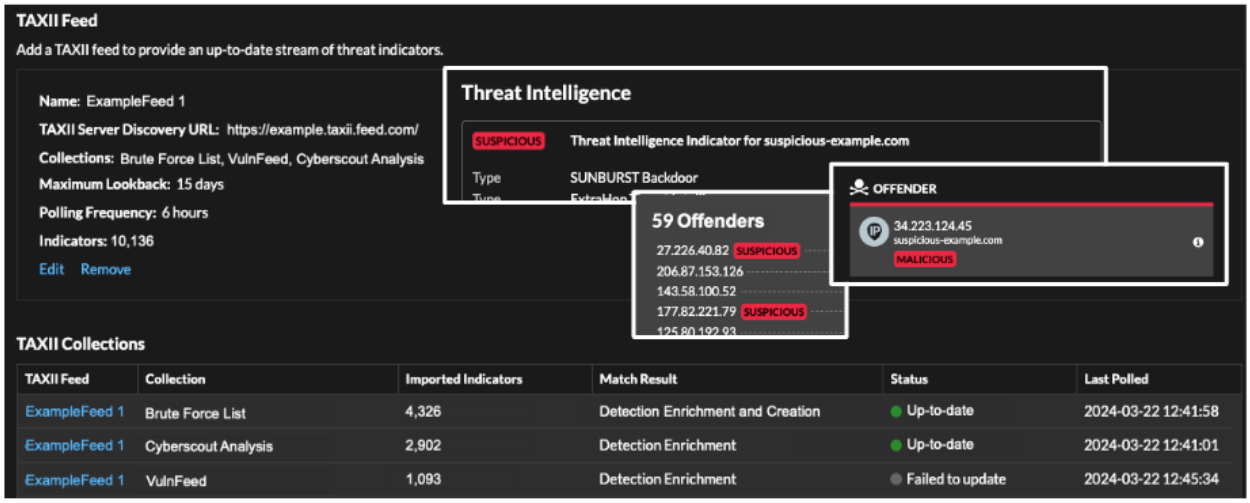
Smart Investigations

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.



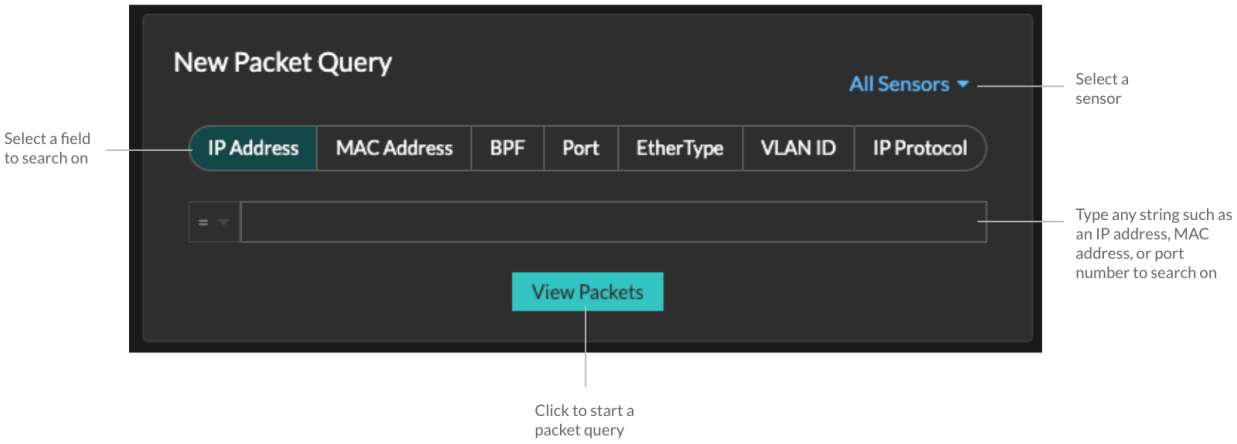
TAXII Feeds

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.



Packets

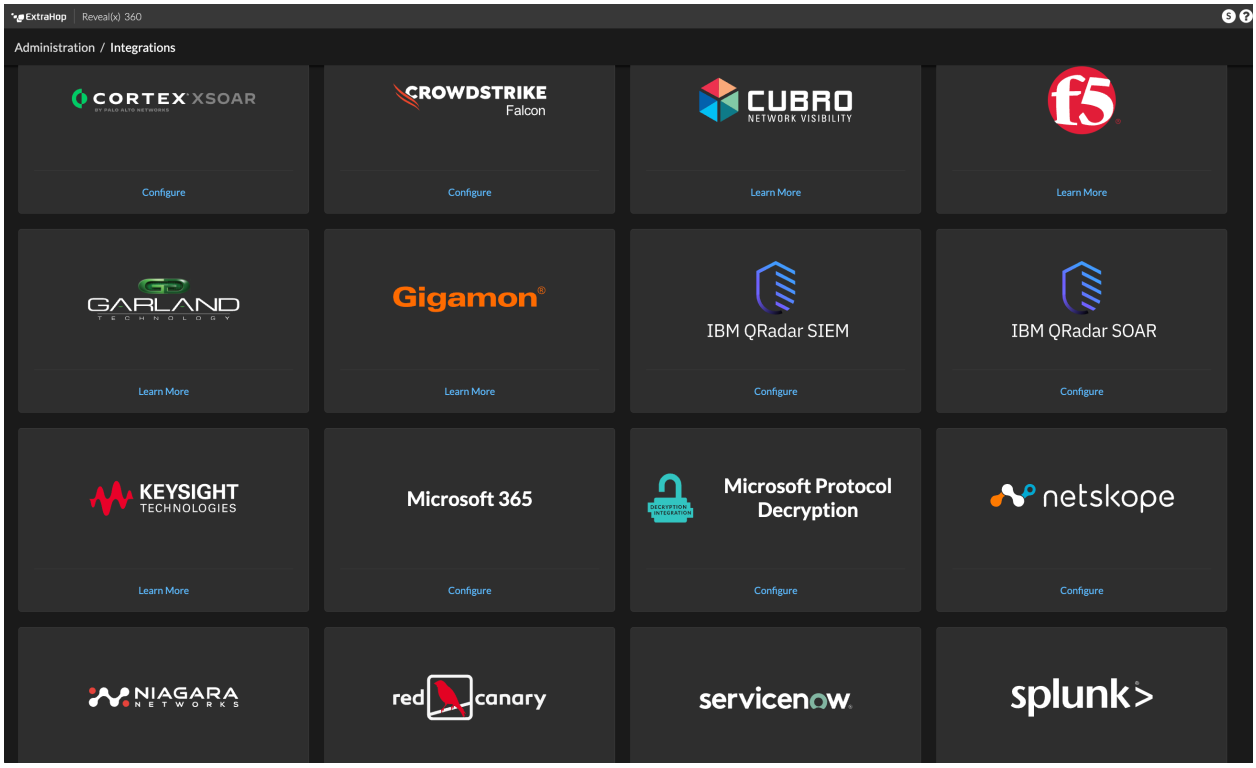
On the Packets page, the New Packet Query window enables you to create a refined query that returns only the results you need.



New 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.