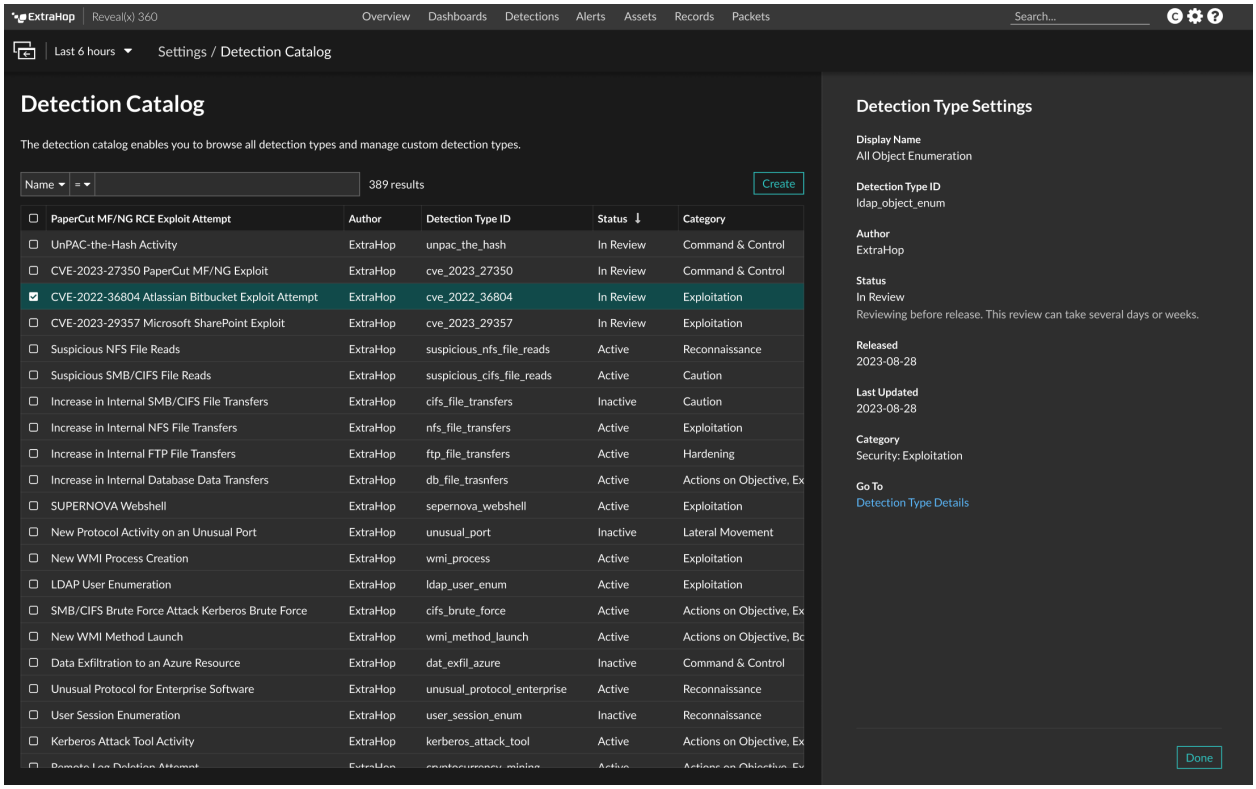
What's New

Published: 2024-01-17

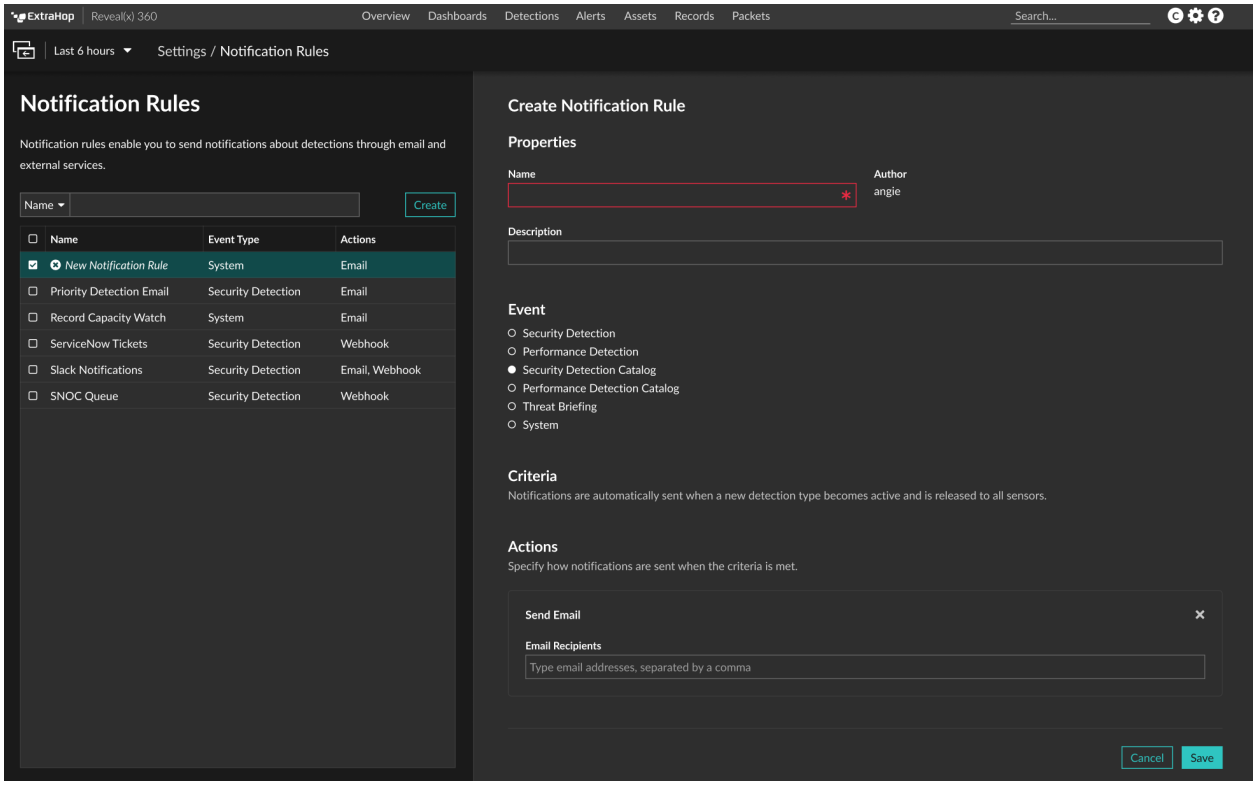
While release notes provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.5.

Detections

The Detection Catalog now identifies whether a detection type is currently available in your environment.

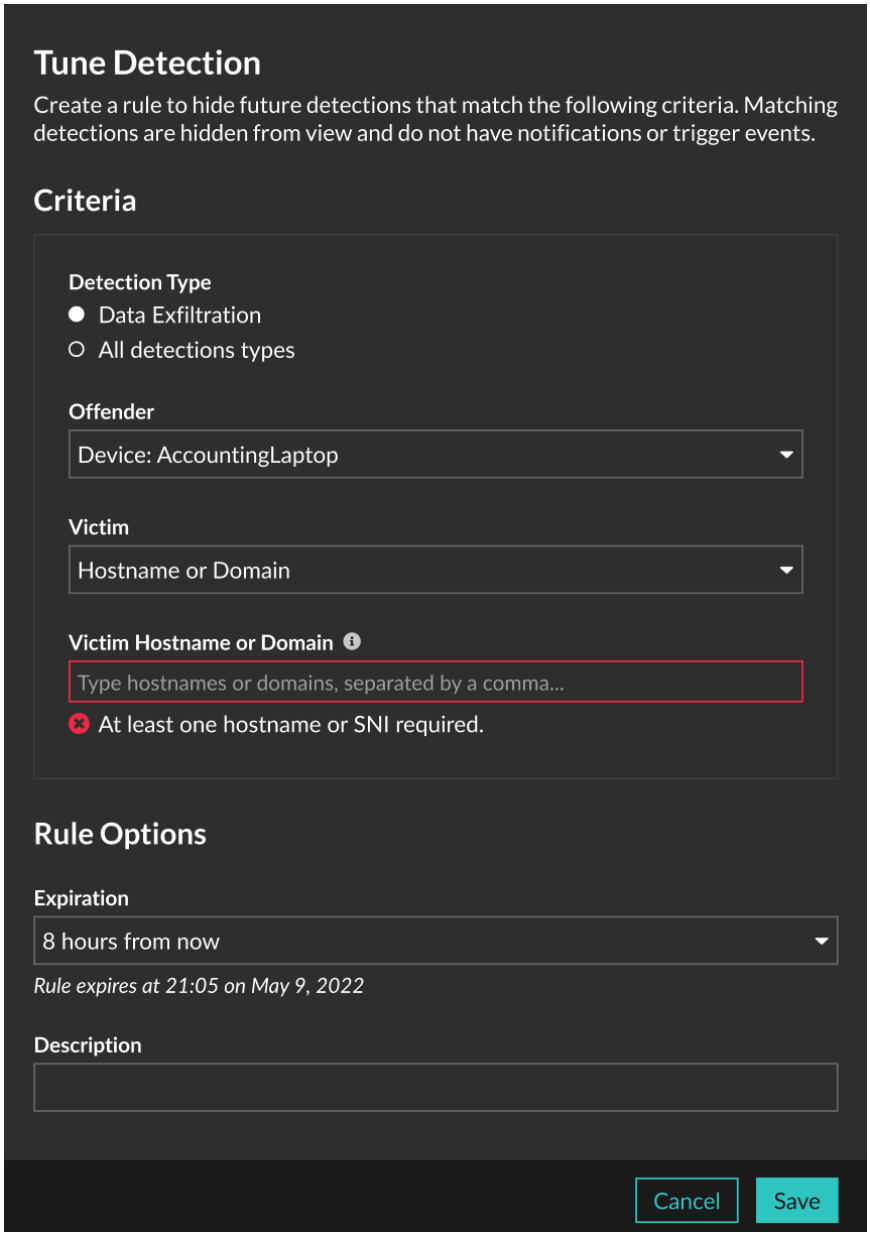


You can also create notifications for the Detection Catalog, which lets you know when detection types are added or updated.



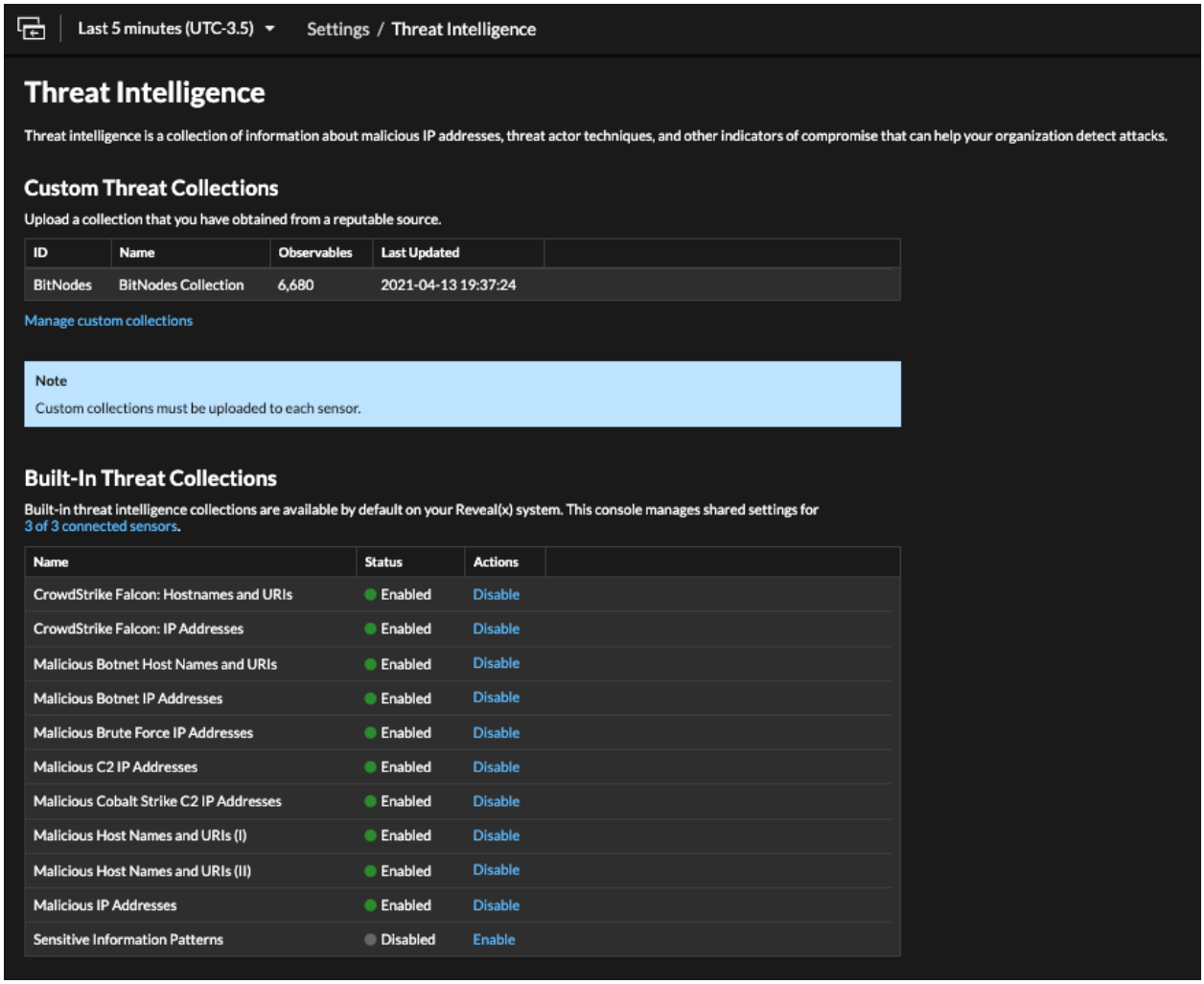
We have also added a Detection Updates guide where you can see when a detection is added or updated.

You can now create tuning rules that hide participants by hostname or domain.



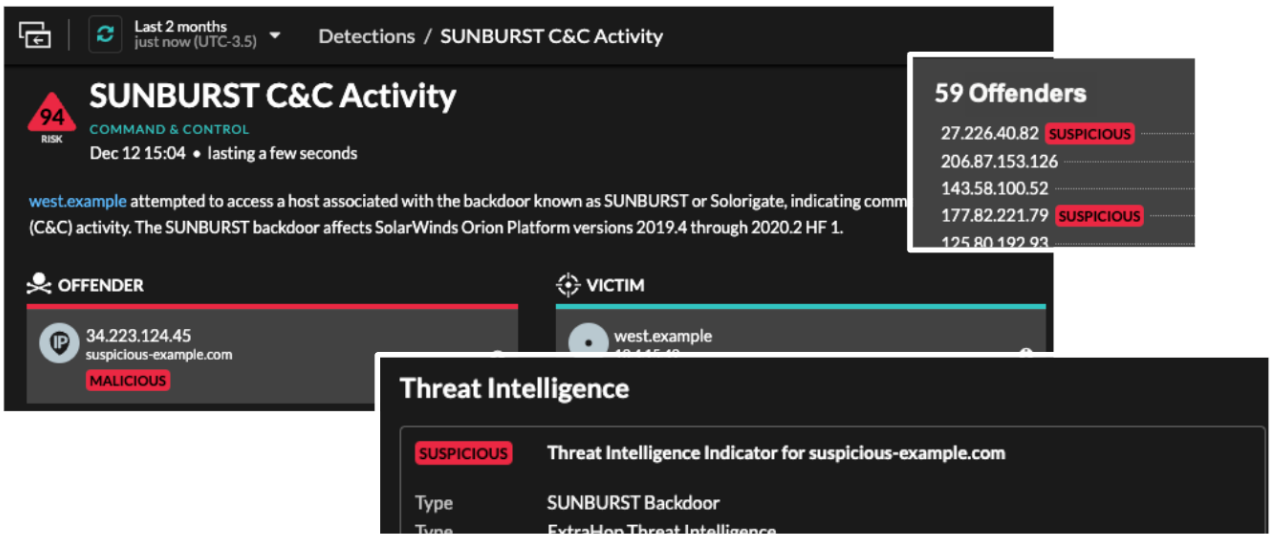
Threat Intelligence

Curated threat collections from CrowdStrike Falcon are now available by default in your ExtraHop system. CrowdStrike threat collections no longer require a CrowdStrike license and can be managed with other ExtraHop built-in collections on the Threat Intelligence page.



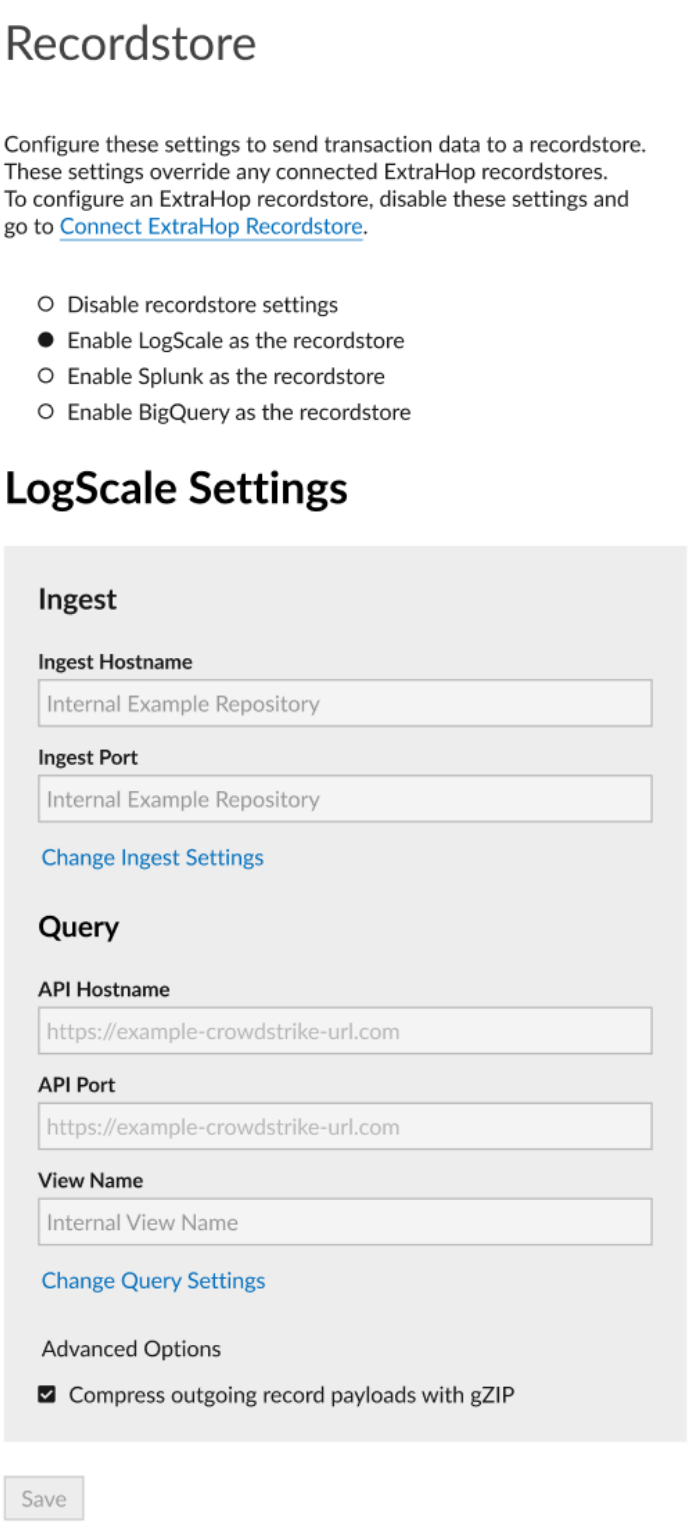
Detections can now be recommended for triage when a participant hostname or IP address is referenced in a threat collection that is enabled on your system.

Detection participants that are associated with suspicious IP addresses or hostnames according to threat intelligence are now labeled in detections and detection type summaries. Matches to high confidence indicators of compromise from built-in CrowdStrike threat collections are labeled as Malicious.

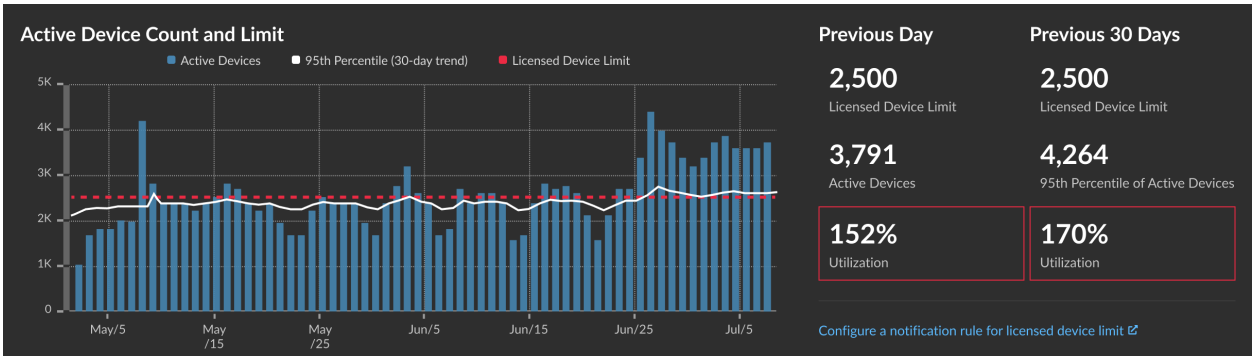


For Administrators

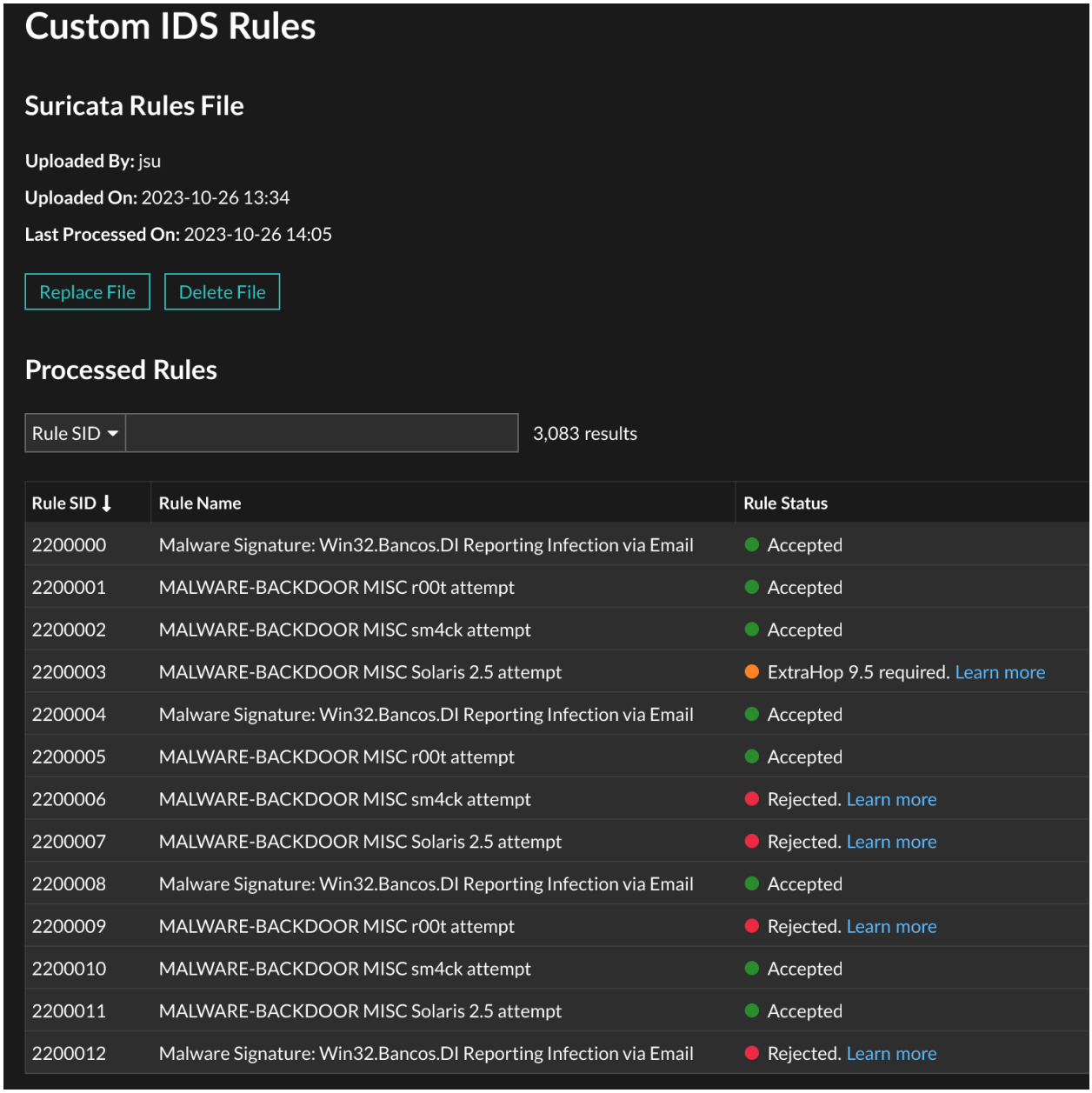
You can now enable CrowdStrike Falcon LogScale as the recordstore. (Requires Reveal(x) Enterprise and an ExtraHop license for the LogScale recordstore.)



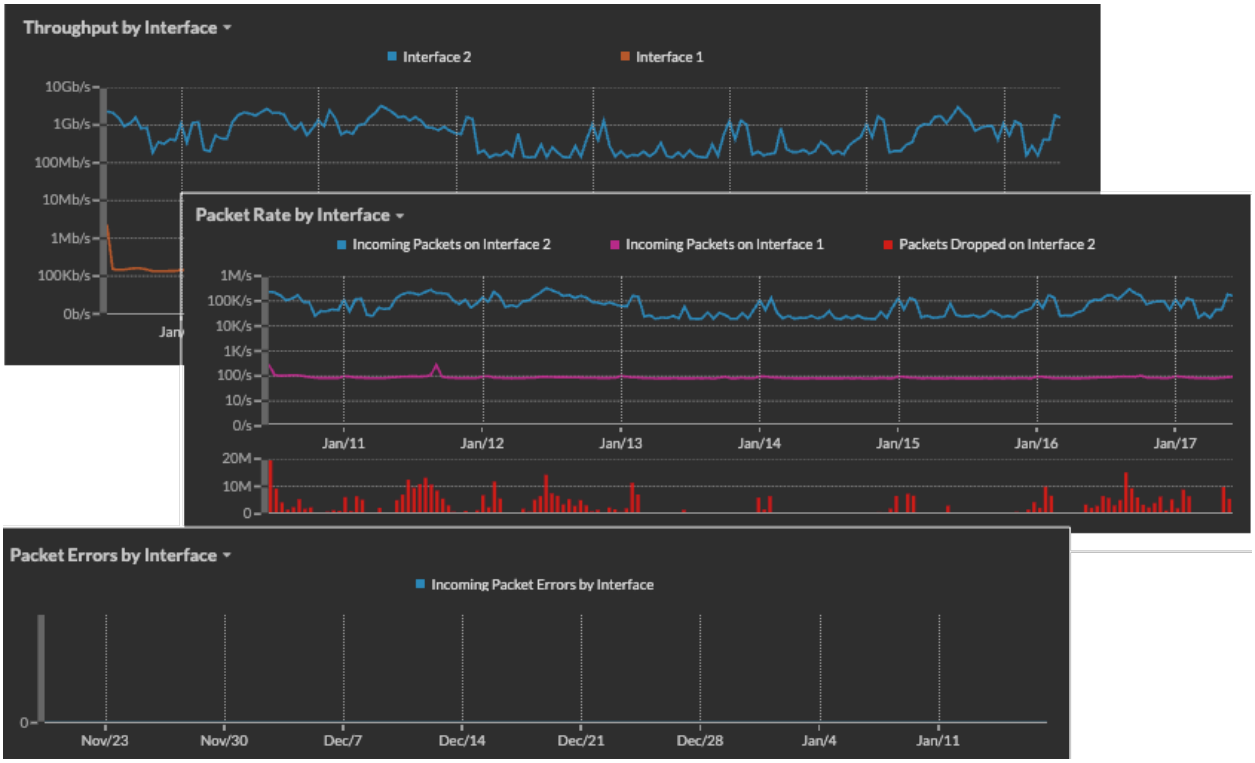
We added new charts to the Administration page for Reveal(x) Enterprise and Reveal(x) 360 that enable you to monitor active device counts and compare them to your licensed limit. You can create a system notification rule to notify Administrators when the active device count reaches a specified threshold.



You can now upload a custom set of IDS rules to IDS sensors that the ExtraHop system converts to detections that you can view and investigate.



We added System Health charts where you can monitor metrics for throughput, packet rate, and packet errors by interface.


Throughput by Interface
Interface 2
Interface 1
10Gb/s
1Gb/s
100Mb/s
10Mb/s
1Mb/s
100Kb/s
0b/s
Packet Rate by Interface
Incoming Packets on Interface 2
Incoming Packets on Interface 1
Packets Dropped on Interface 2
1M/s
100K/s
10K/s
1K/s
100/s
10/s
0/s
Jan/11
Jan/12
Jan/13
Jan/14
Jan/15
Jan/16
Jan/17
20M
10M
0
Packet Errors by Interface
Incoming Packet Errors by Interface
0
Nov/23
Nov/30
Dec/7
Dec/14
Dec/21
Dec/28
Jan/4
Jan/11