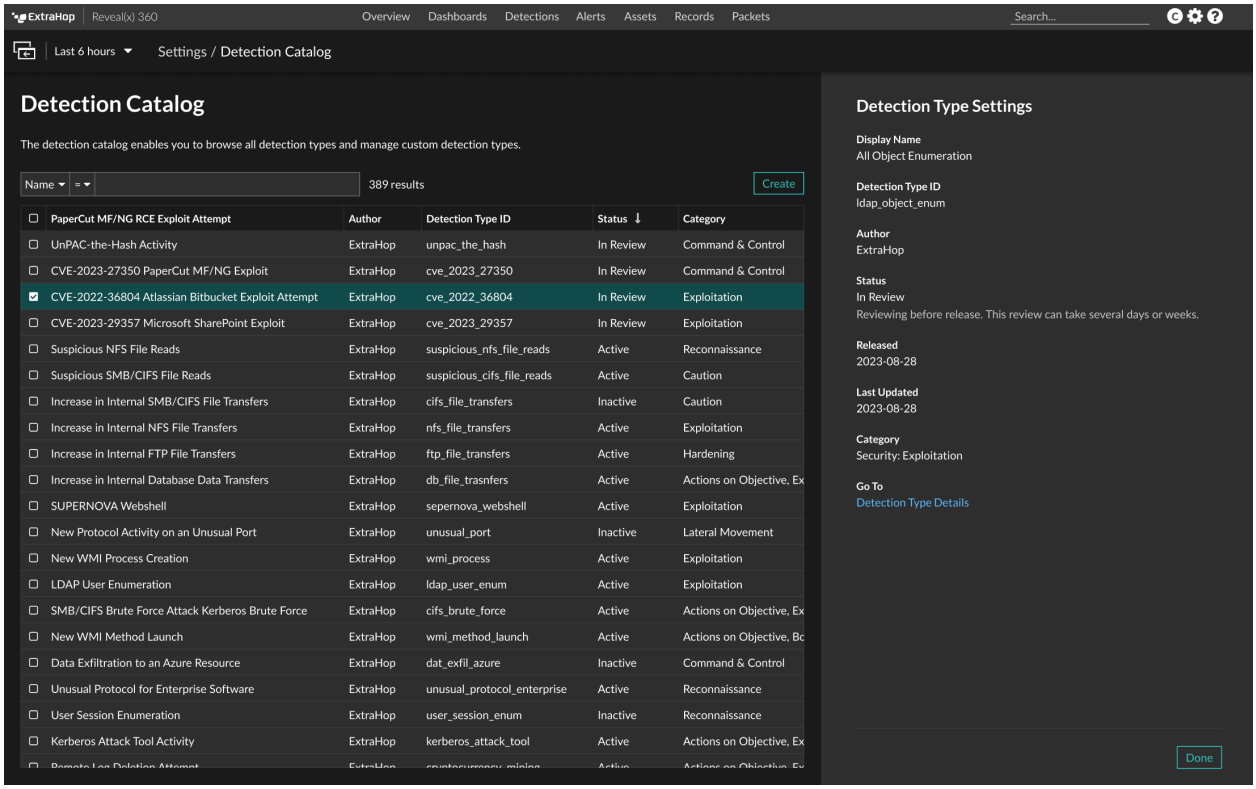
Was ist neu

Veröffentlicht: 2024-01-22

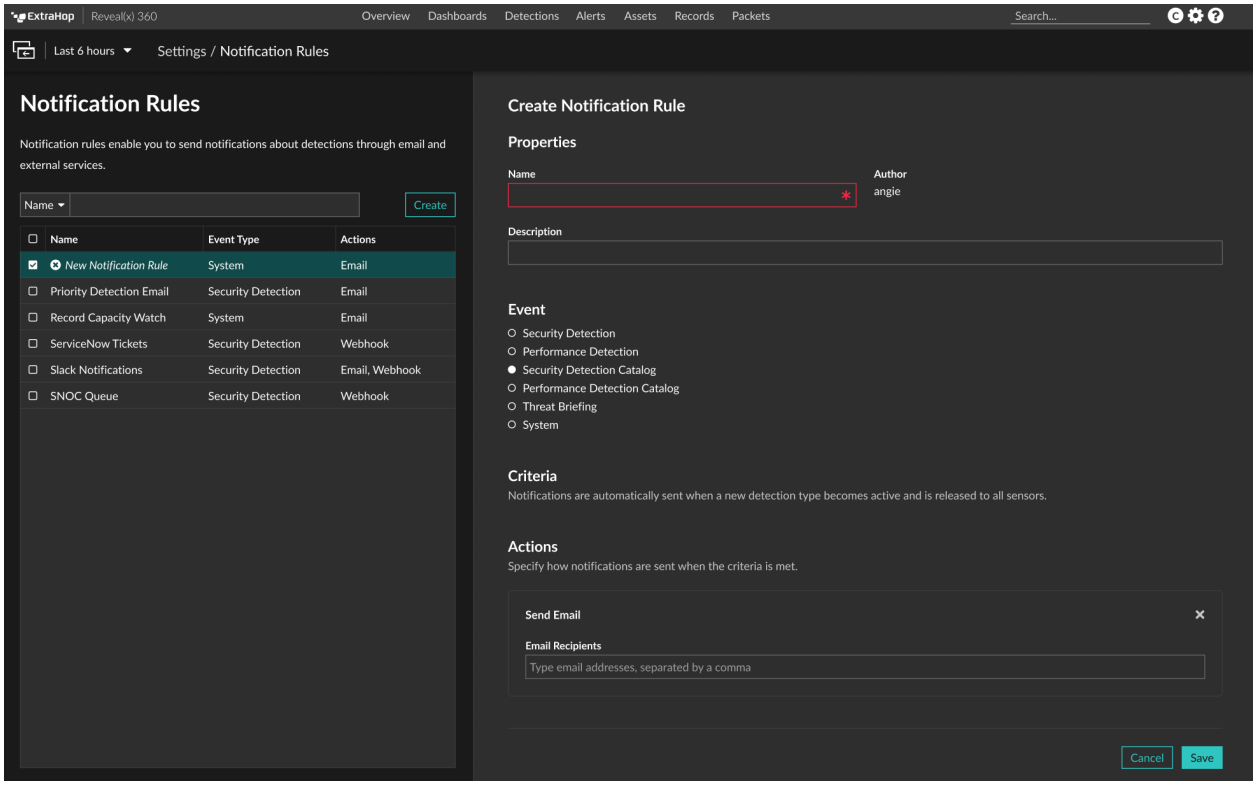
Während Versionshinweise geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.5.

Erkennungen

Das Erkennungskatalog identifiziert jetzt, ob ein Erkennungstyp derzeit in Ihrer Umgebung verfügbar ist.

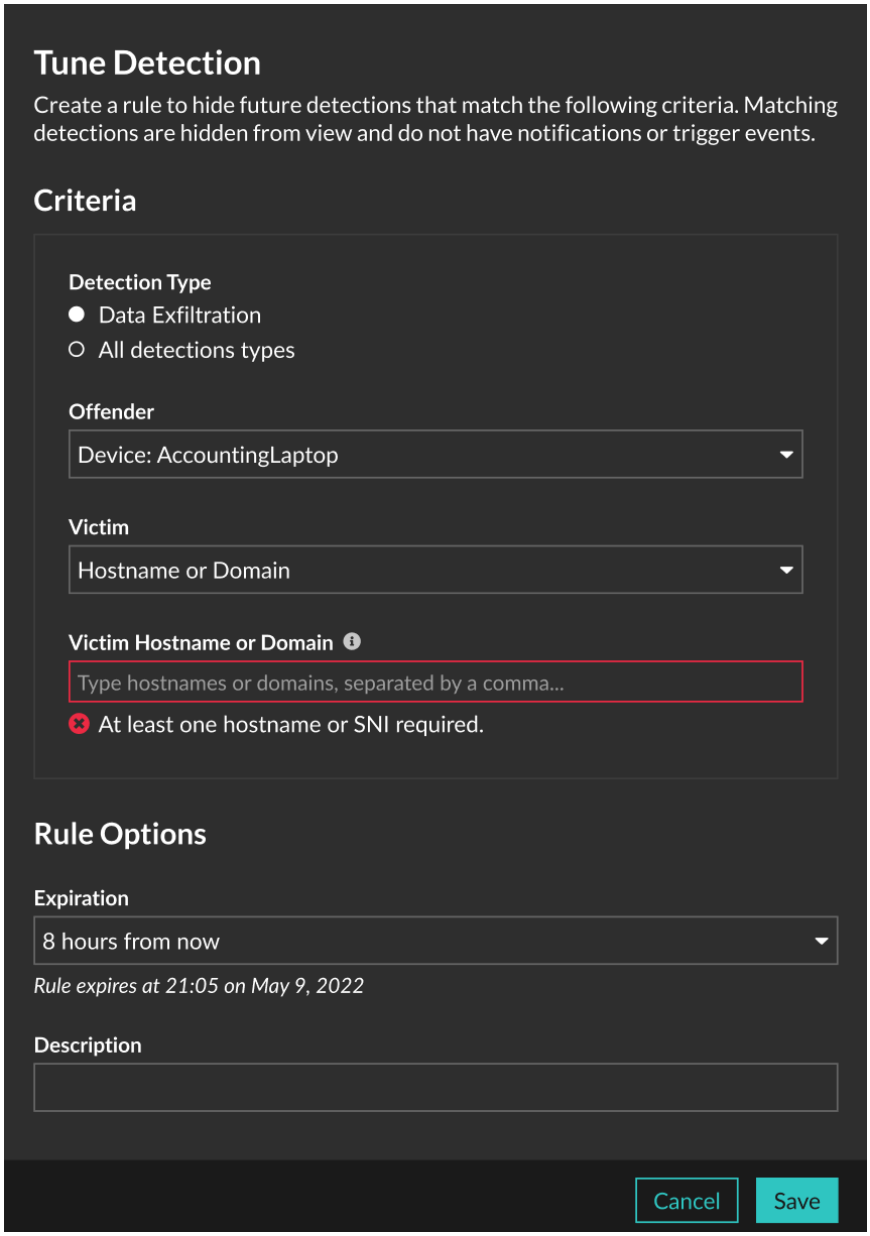


Du kannst auch Benachrichtigungen für den Erkennungskatalog erstellen, das Sie darüber informiert, wenn Erkennungstypen hinzugefügt oder aktualisiert werden.



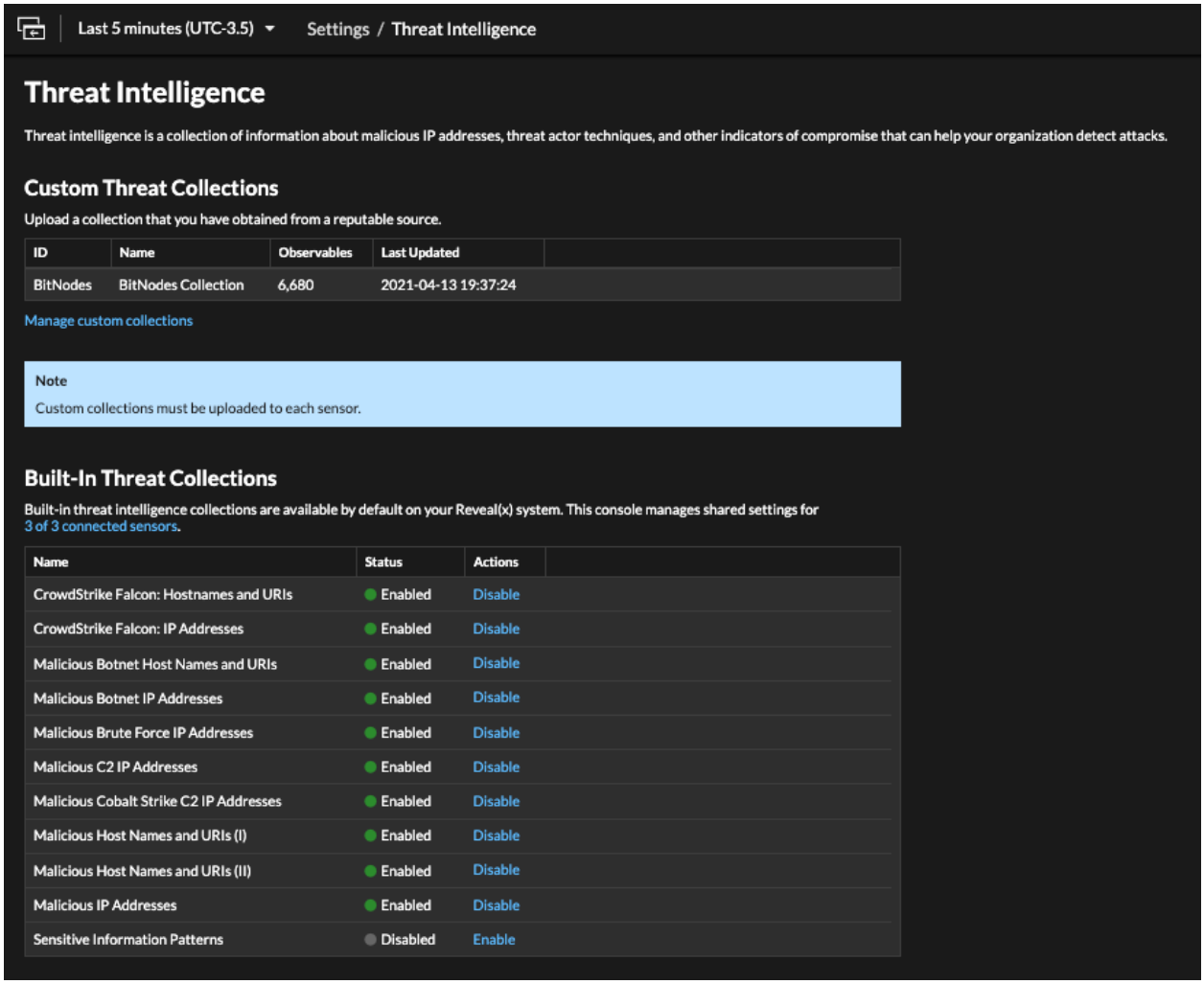
Wir haben auch eine hinzugefügt Leitfaden zu Erkennungsaktualisierungen wo Sie sehen können, wann eine Erkennung hinzugefügt oder aktualisiert wird.

Sie können jetzt erstellen Tuning-Regeln die Teilnehmer nach Hostname oder Domain verstecken.



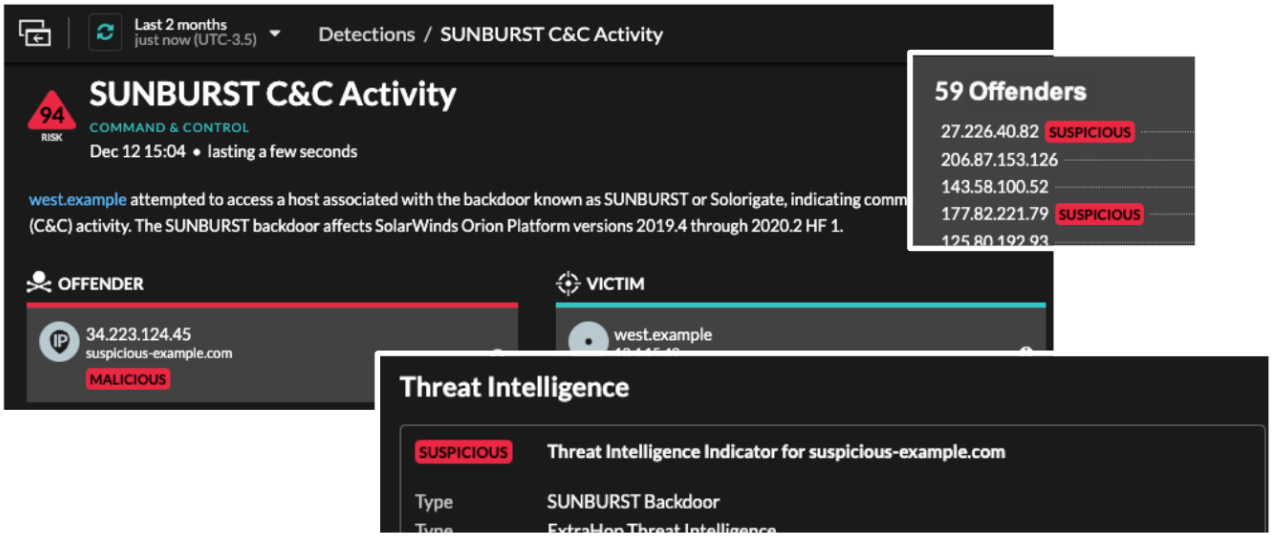
Bedrohungsinformationen

Kuratierte Bedrohungssammlungen von CrowdStrike Falcon sind jetzt standardmäßig in Ihrem ExtraHop-System verfügbar. CrowdStrike-Bedrohungssammlungen benötigen keine CrowdStrike-Lizenz mehr und können mit anderen integrierten ExtraHop-Sammlungen auf dem Seite „Threat Intelligence“.



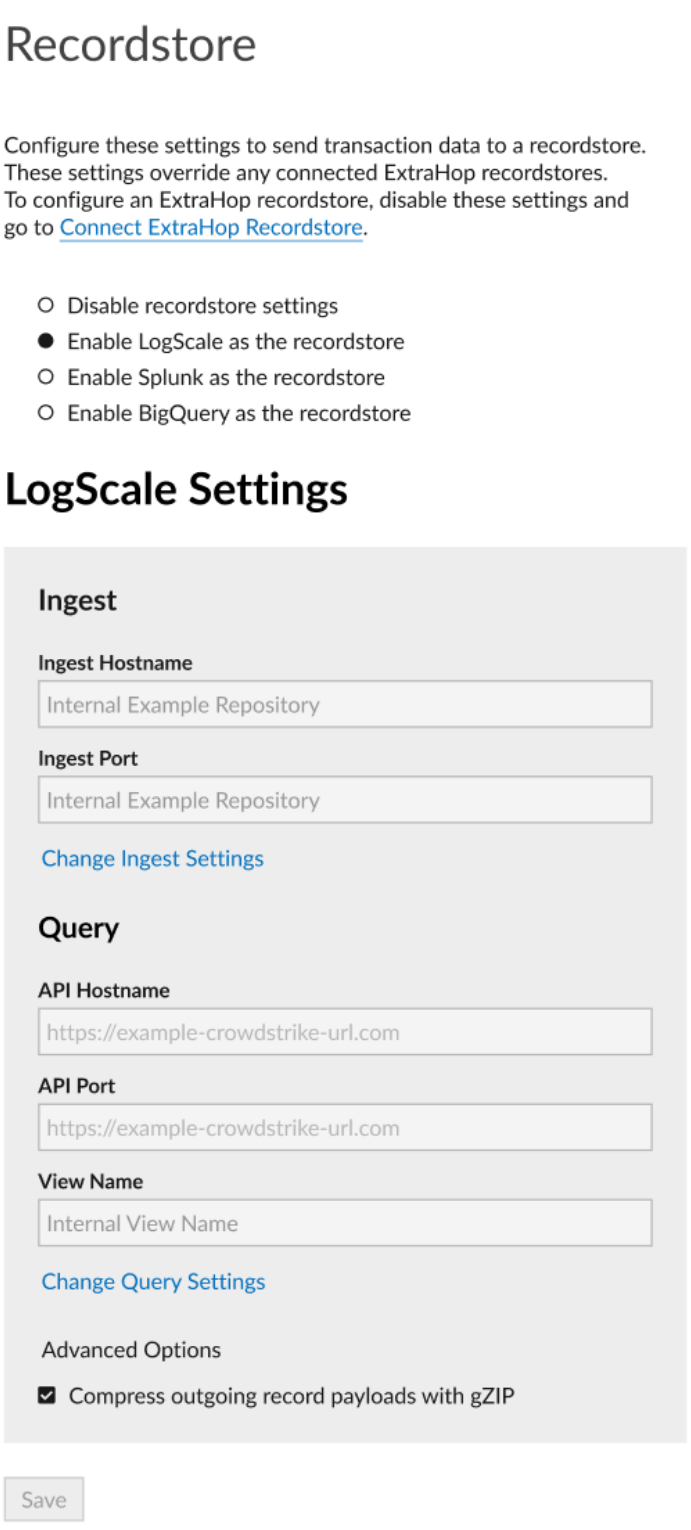
Erkennungen können jetzt für die Triage empfohlen werden wenn der Hostname oder die IP-Adresse eines Teilnehmer in einer Bedrohungssammlung referenziert das ist auf Ihrem System aktiviert.

Erkennungsteilnehmer, die mit verdächtigen IP-Adressen oder Hostnamen verknüpft sind, gemäß Bedrohungsinformationen sind jetzt in Erkennungen und Zusammenfassungen der Erkennungstypen gekennzeichnet. Übereinstimmungen mit Bedrohungsindikatoren mit hoher Konfidenz aus den integrierten CrowdStrike-Bedrohungssammlungen werden als bösartig eingestuft.

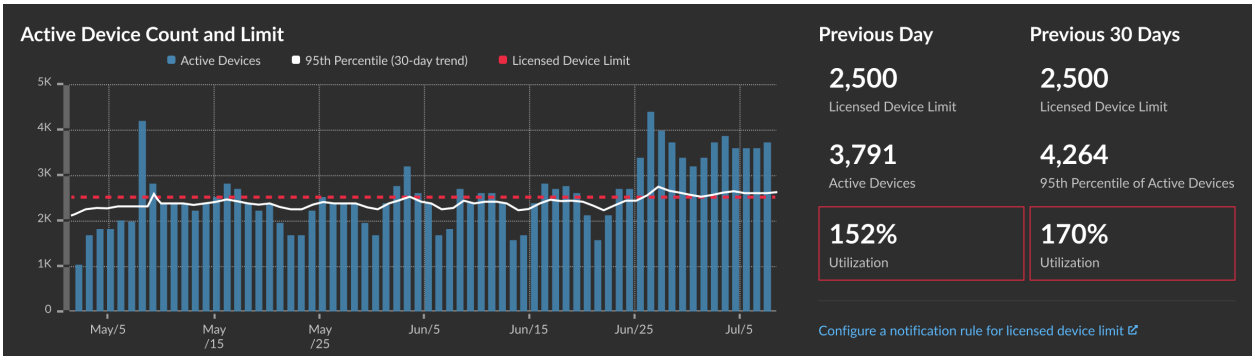


Für Administratoren

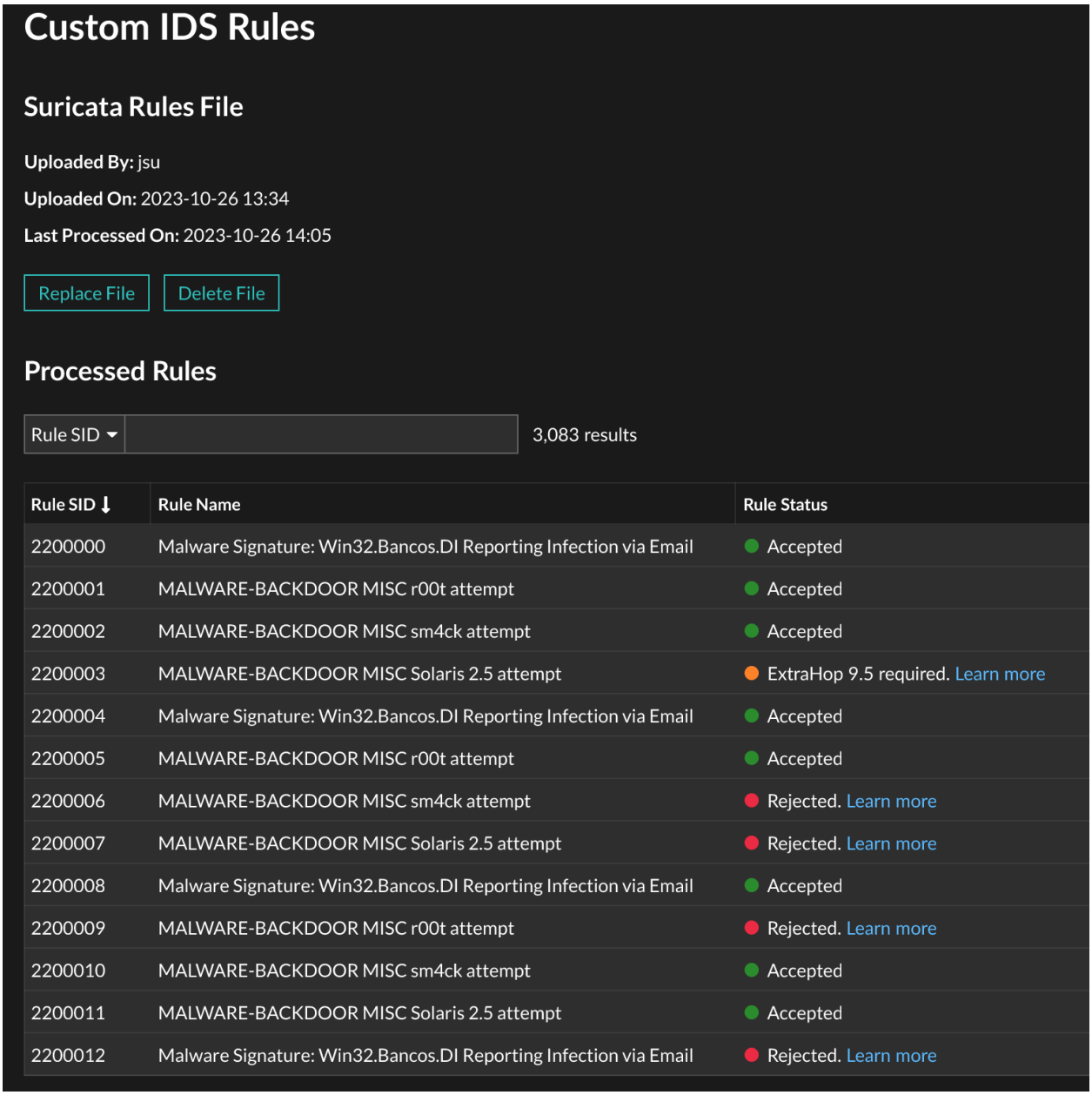
Du kannst jetzt aktiviere CrowdStrike Falcon LogScale wie der Recordstore. (Erfordert Reveal (x) Enterprise und eine ExtraHop-Lizenz für den LogScale Recordstore.)



Wir haben der Administrationsseite neue Charts hinzugefügt für Enthülle (x) Enterprise und Zeige (x) 360 die es Ihnen ermöglichen, die Anzahl der aktiven Gerät zu überwachen und sie mit Ihrem Lizenzlimit zu vergleichen. Du kannst eine Regel für Systembenachrichtigungen erstellen um Administratoren zu benachrichtigen, wenn die Anzahl der aktiven Gerät einen bestimmten Schwellenwert erreicht.

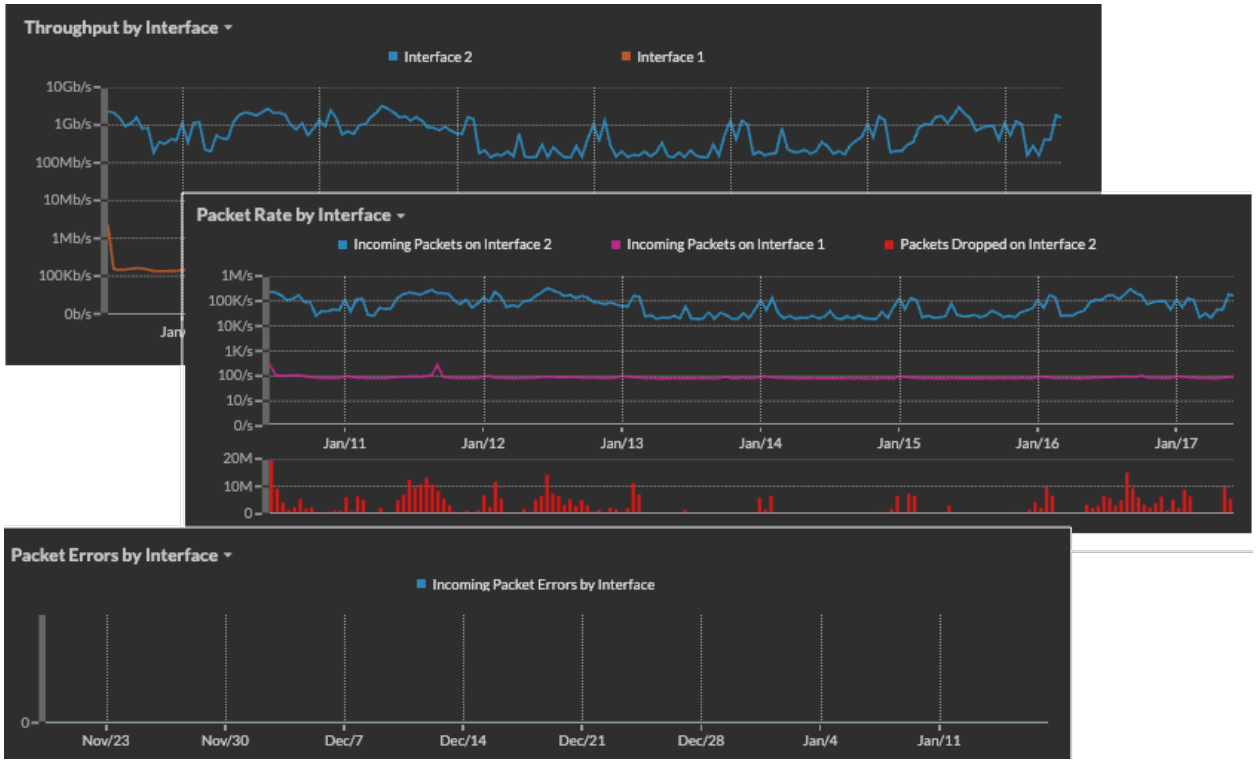


Du kannst jetzt Laden Sie einen benutzerdefinierten Satz von IDS-Regeln auf IDS-Sensoren hoch die das ExtraHop-System in Erkennungen umwandelt, die Sie einsehen und untersuchen können.



Rule SID	Rule Name	Rule Status
2200000	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200001	MALWARE-BACKDOOR MISC r00t attempt	Accepted
2200002	MALWARE-BACKDOOR MISC sm4ck attempt	Accepted
2200003	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	ExtraHop 9.5 required. Learn more
2200004	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200005	MALWARE-BACKDOOR MISC r00t attempt	Accepted
2200006	MALWARE-BACKDOOR MISC sm4ck attempt	Rejected. Learn more
2200007	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	Rejected. Learn more
2200008	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200009	MALWARE-BACKDOOR MISC r00t attempt	Rejected. Learn more
2200010	MALWARE-BACKDOOR MISC sm4ck attempt	Accepted
2200011	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	Accepted
2200012	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Rejected. Learn more

Wir Diagramme zum Systemzustand hinzugefügt wo Sie Metriken für Durchsatz, Paketrate und Paketfehler nach Schnittstelle überwachen können.


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