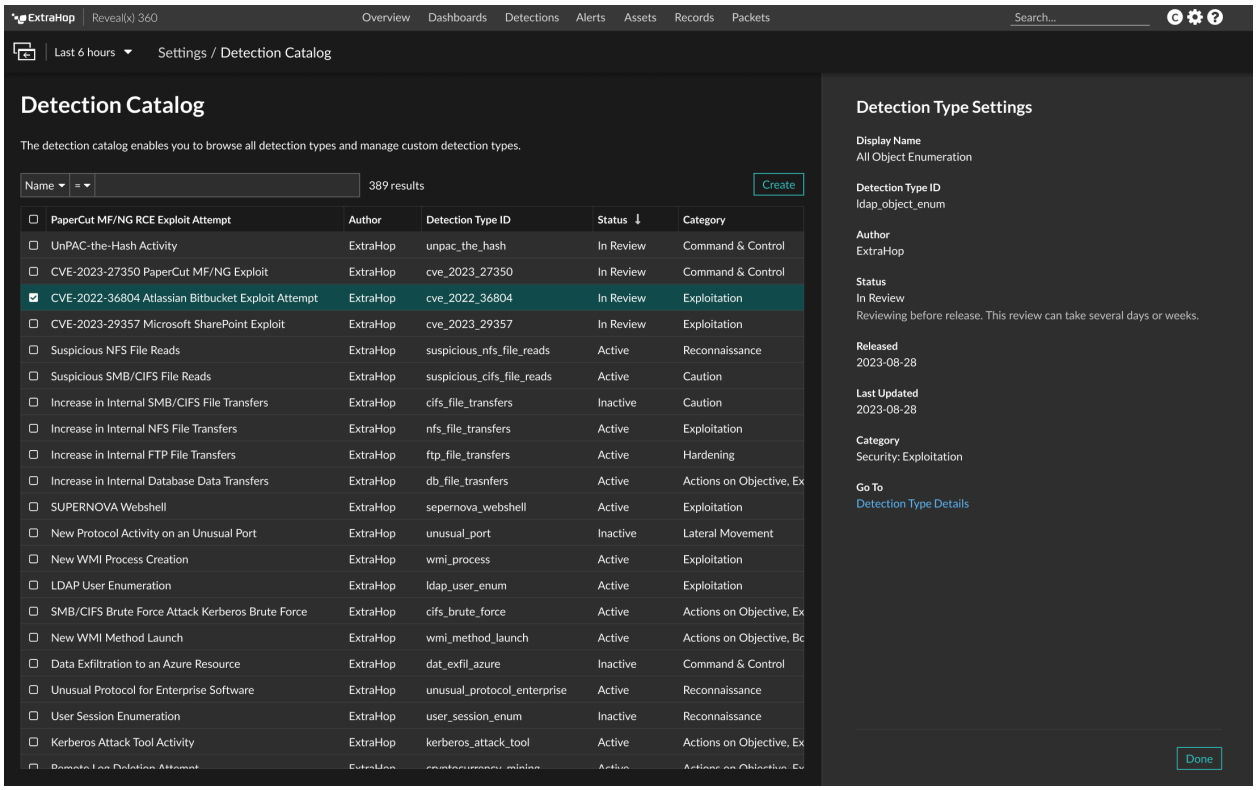
Quoi de neuf

Publié: 2024-01-23

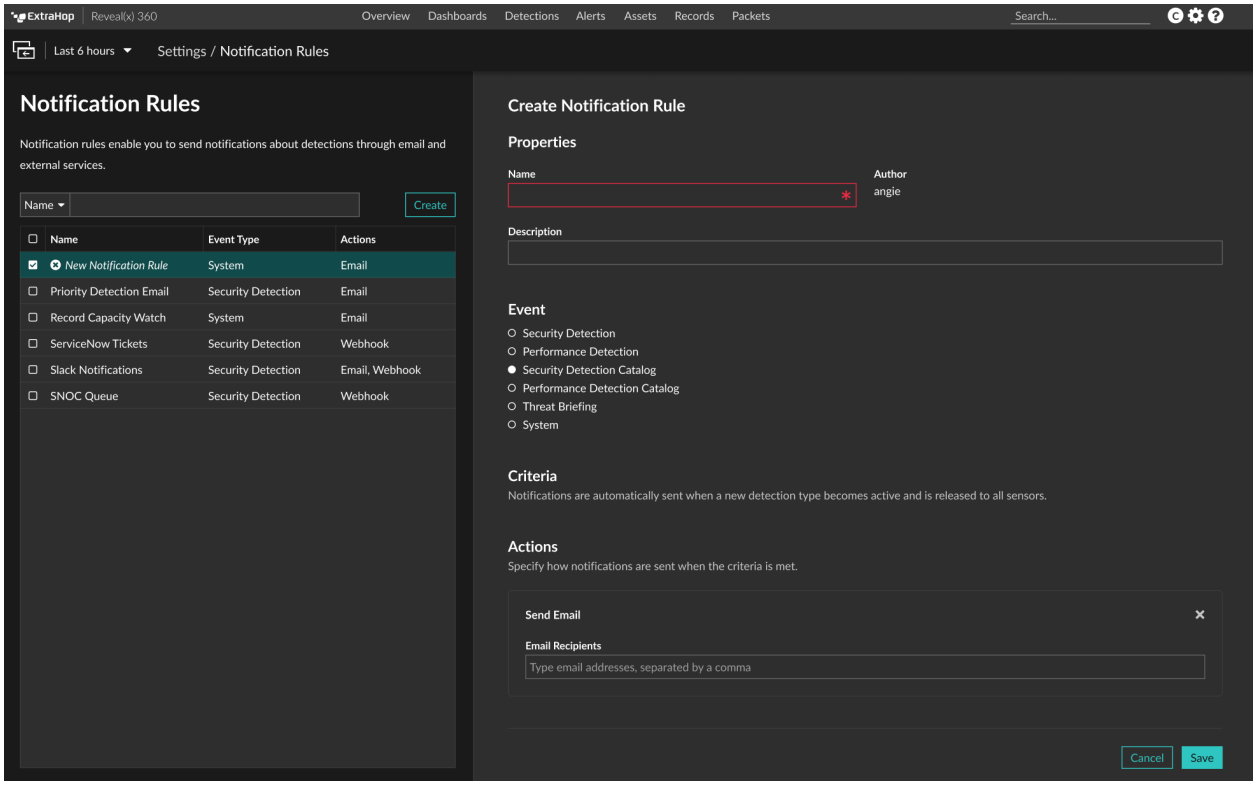
Alors que notes de version pour un aperçu complet de nos mises à jour de versions, voici un aperçu des fonctionnalités les plus intéressantes d'ExtraHop 9.5.

Détections

Le Catalogue de détection identifie désormais si un type de détection est actuellement disponible dans votre environnement.

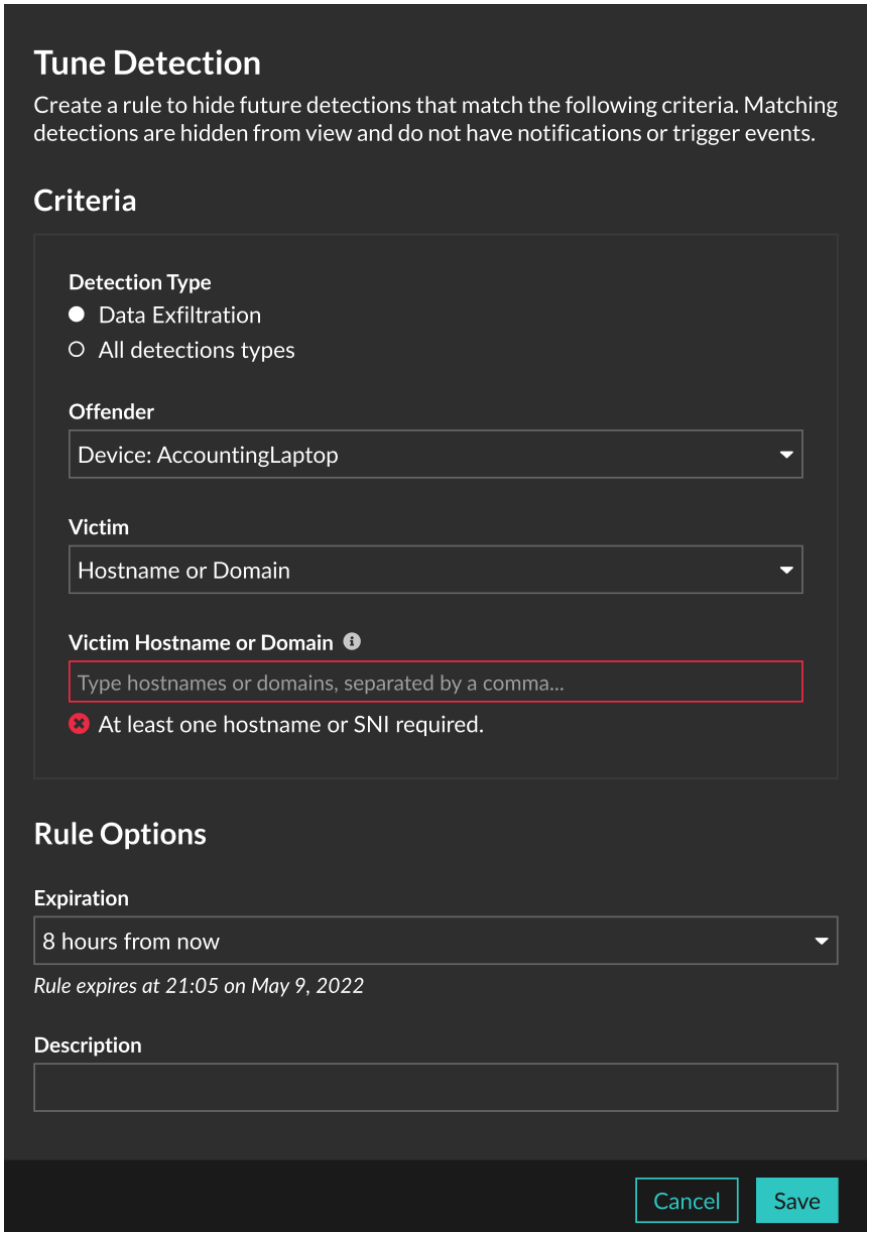


Vous pouvez également créer des notifications pour le catalogue de détection, qui vous permet de savoir quand des types de détection sont ajoutés ou mis à jour.



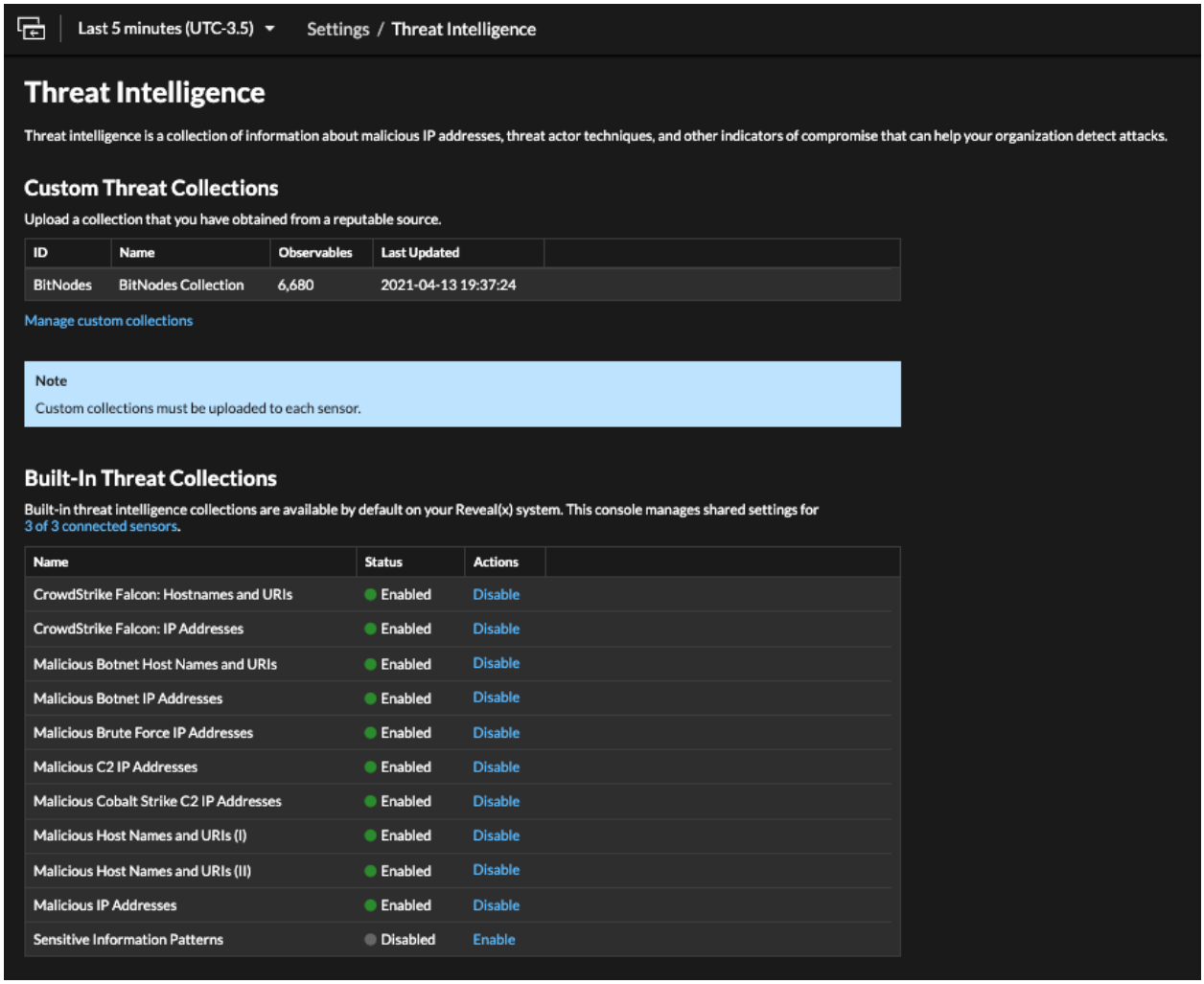
Nous avons également ajouté un Guide des mises à jour de détection où vous pouvez voir quand une détection est ajoutée ou mise à jour.

Vous pouvez désormais créer règles d'exceptions qui masquent les participants par nom d'hôte ou domaine.



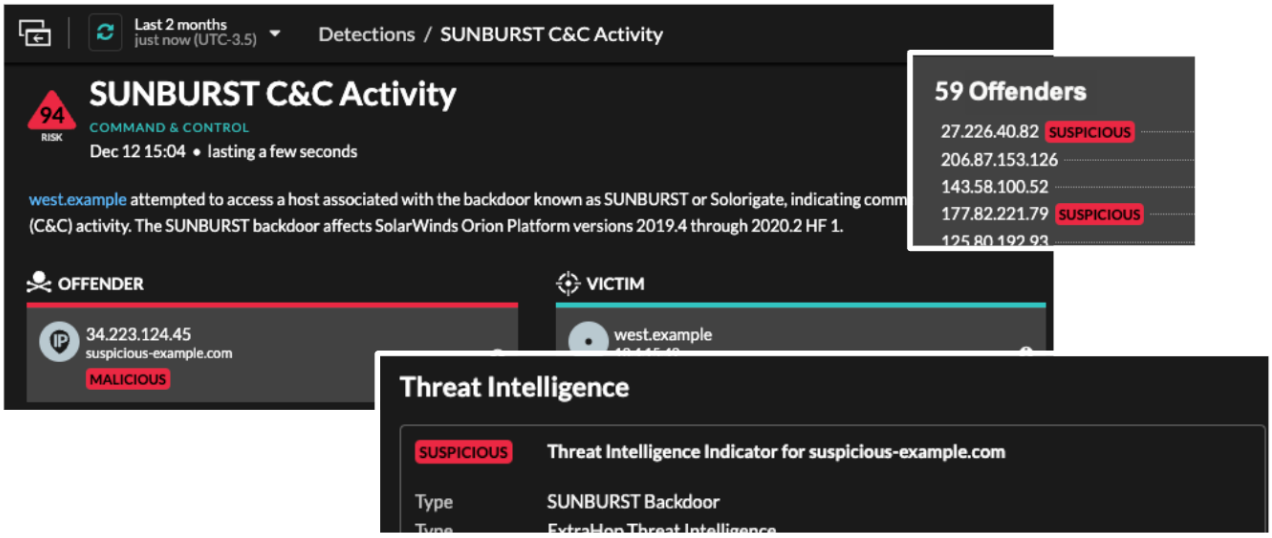
Renseignements sur les menaces

Collections de menaces sélectionnées de CrowdStrike Falçon sont désormais disponibles par défaut dans votre système ExtraHop. Les collections de menaces CrowdStrike ne nécessitent plus de licence CrowdStrike et peuvent être gérées à l'aide d'autres collections intégrées d'ExtraHop sur Page relative au renseignement sur les menaces.



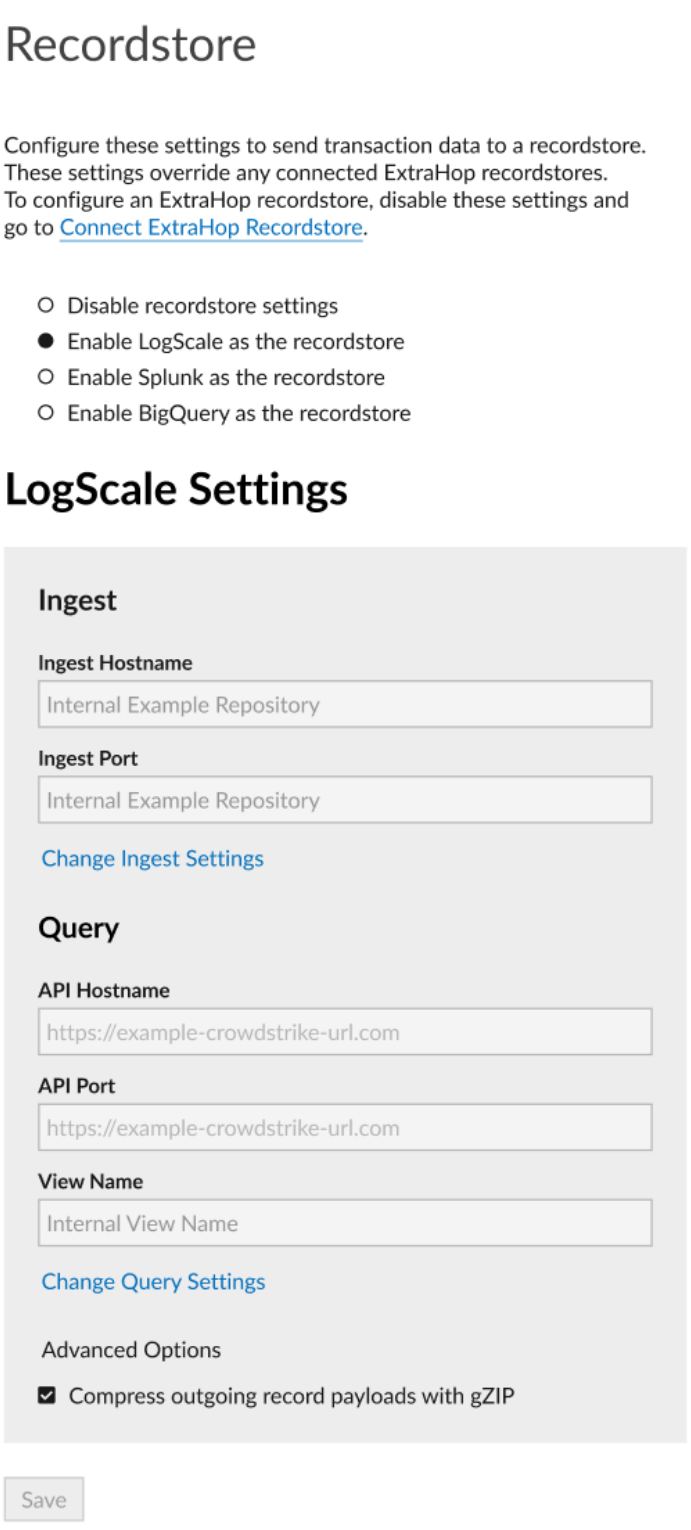
Les détections peuvent désormais être recommandé pour le triage lorsque le nom d'hôte ou l'adresse IP d'un participant est référencé dans une collecte des menaces qui est activé sur votre système.

Détection des participants associés à des adresses IP ou à des noms d'hôte suspects selon renseignements sur les menaces sont désormais étiquetés dans les détections et les résumés des types de détection. Les correspondances avec des indicateurs de compromission à haut niveau de confiance provenant des collections de menaces intégrées à CrowdStrike sont qualifiées de malveillantes.

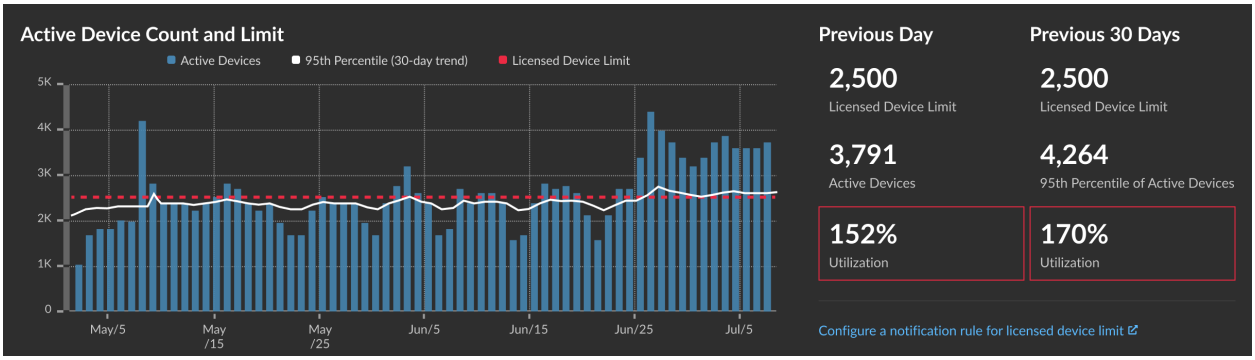


Pour les administrateurs

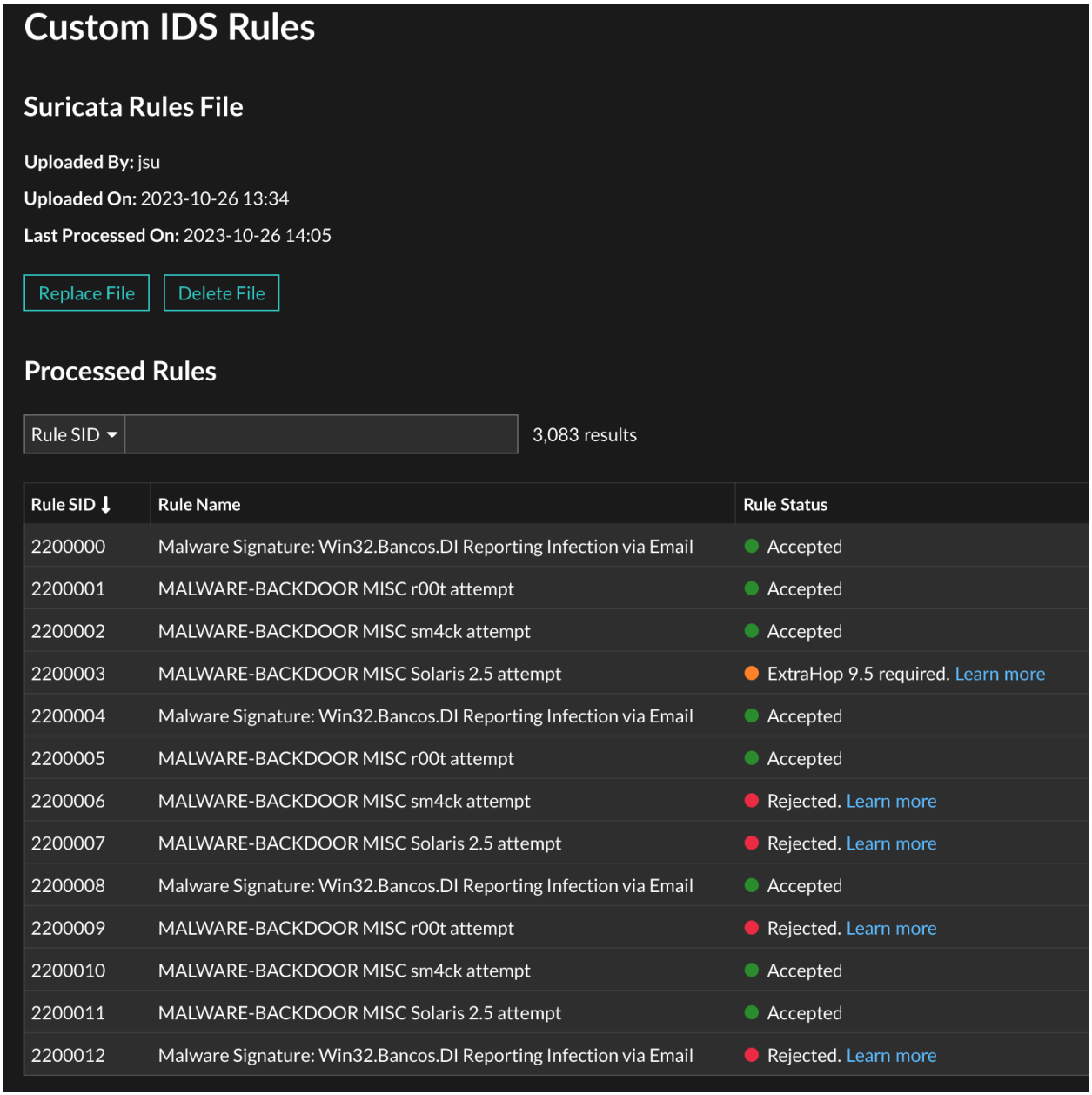
Tu peux maintenant activer CrowdStrike Falçon LogScale comme espace de stockage des enregistrements. (Nécessite Reveal (x) Enterprise et une licence ExtraHop pour l'espace de stockage des enregistrements LogScale.)



Nous avons ajouté de nouveaux graphiques à la page Administration pour Reveal (x) Enterprise et Révéler (x) 360 qui vous permettent de surveiller le nombre d'équipements actifs et de le comparer à la limite de votre licence. Tu peux créer une règle de notification système pour avertir les administrateurs lorsque le nombre d'équipements actifs atteint un seuil défini.

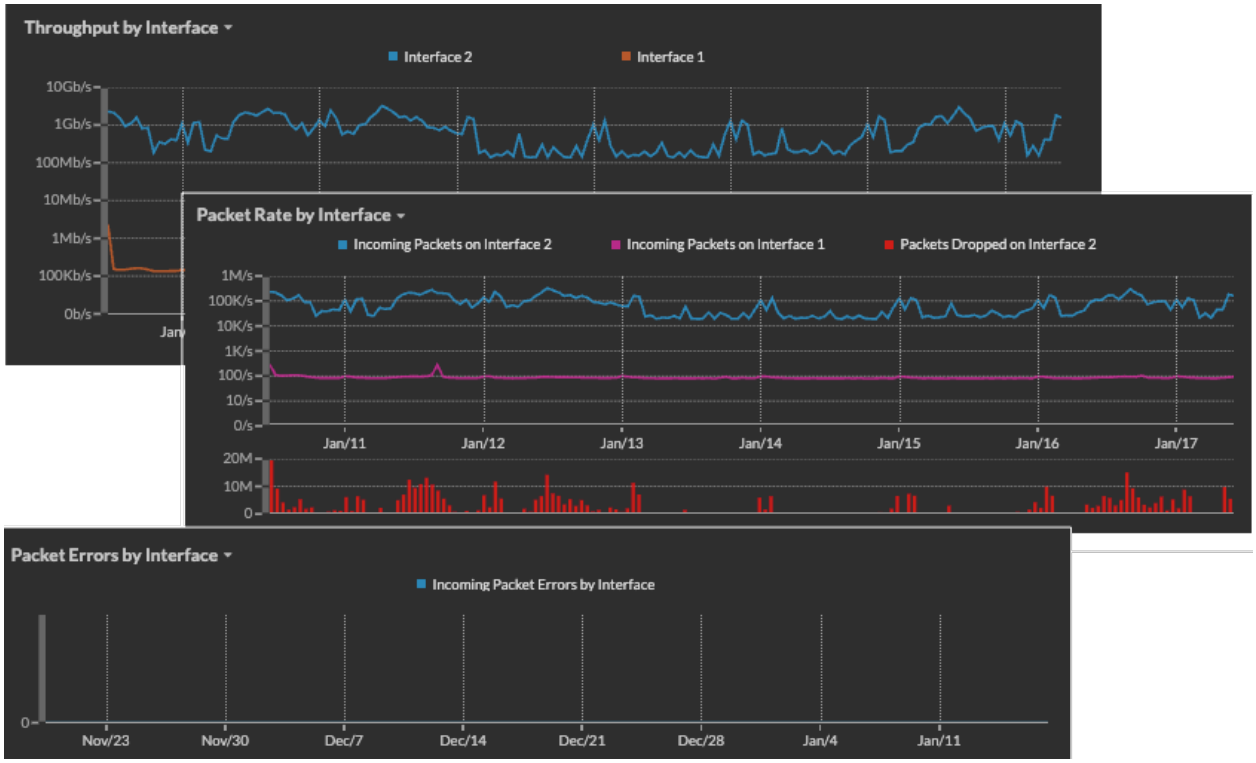


Tu peux maintenant télécharger un ensemble personnalisé de règles IDS vers les capteurs IDS que le système ExtraHop convertit en détections que vous pouvez consulter et examiner.



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

Nous graphiques de santé du système ajoutés où vous pouvez surveiller les mesures relatives au débit, au débit de paquets et aux erreurs de paquets par 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