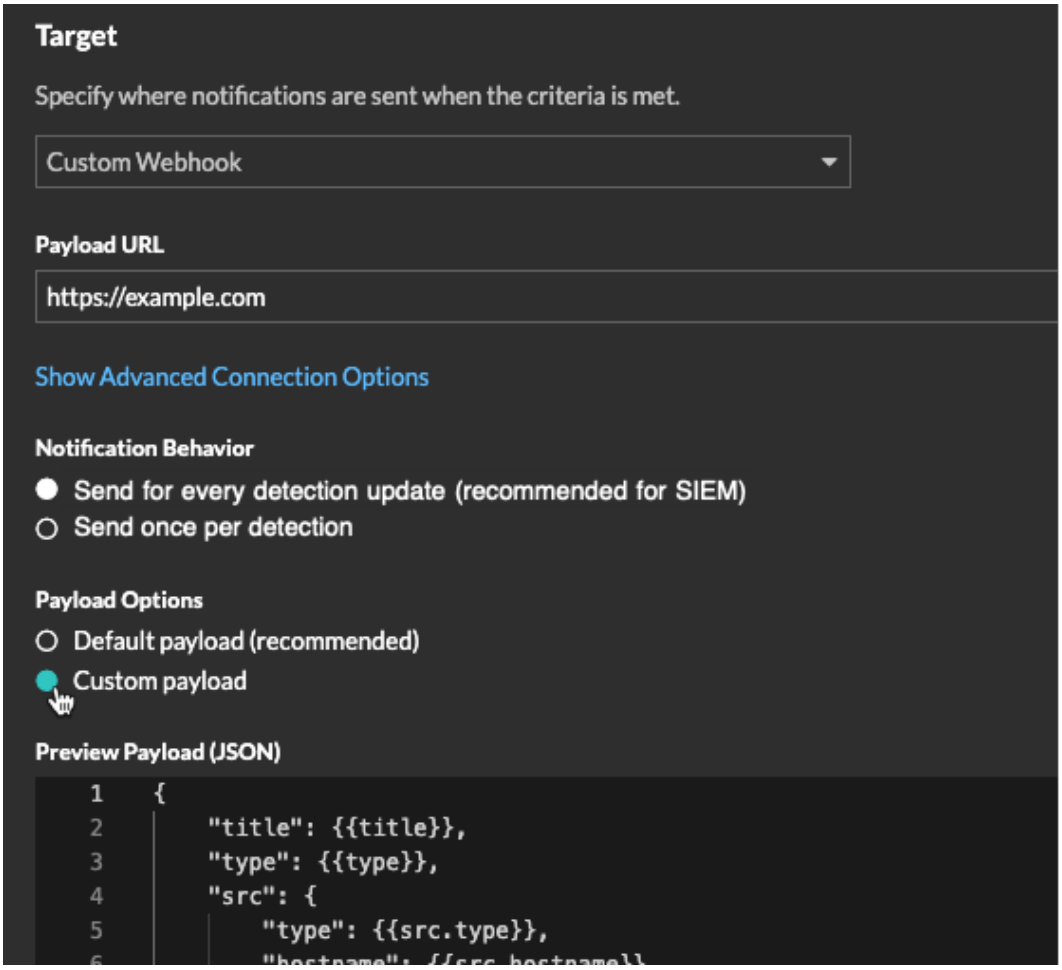
Quoi de neuf

Publié: 2024-10-26

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 9.8.

Notifications de détection améliorées

Les détections et les notifications de détection ont été optimisées pour l'exportation de données de détection granulaires. Les utilisateurs peuvent désormais configurer les règles de notification pour envoyer une charge utile de webhook par défaut ou personnalisée pour chaque mise à jour de détection, ou envoyer une seule notification pour chaque détection.

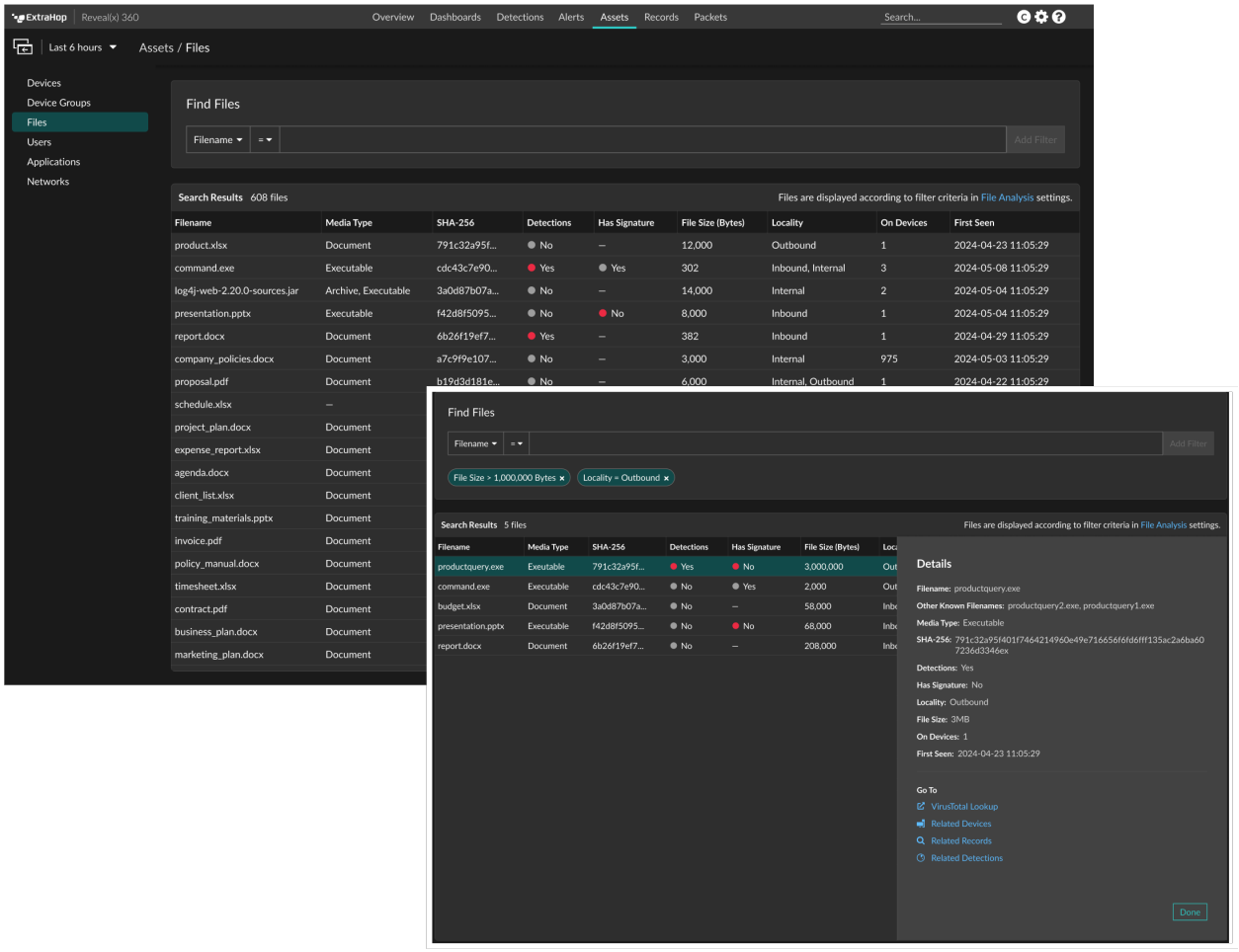


Rapport sur les opérations de sécurité

Vous pouvez désormais sélectionner le contenu à inclure dans Rapport sur les opérations de sécurité que vous générez à partir d'une page d'aperçu.

Page Nouveaux fichiers

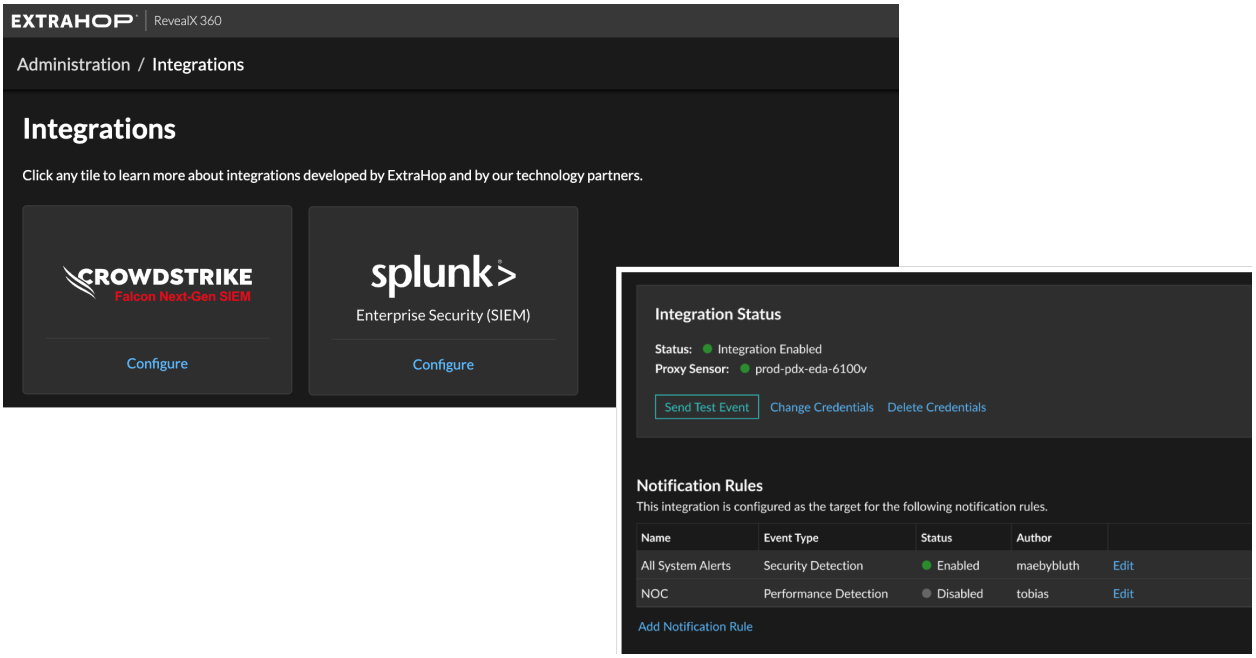
Le Page des fichiers affiche un tableau des fichiers hachés en fonction de filtres configurés et activés à partir des paramètres d'analyse des fichiers. Les détails des fichiers vous permettent d'étudier plus en détail le hachage des fichiers SHA-256 dans les appareils, les enregistrements, les détections et VirusTotal Lookup, un outil tiers.



Nouvelles intégrations avec RevealX 360

Intégrations SIEM de nouvelle génération

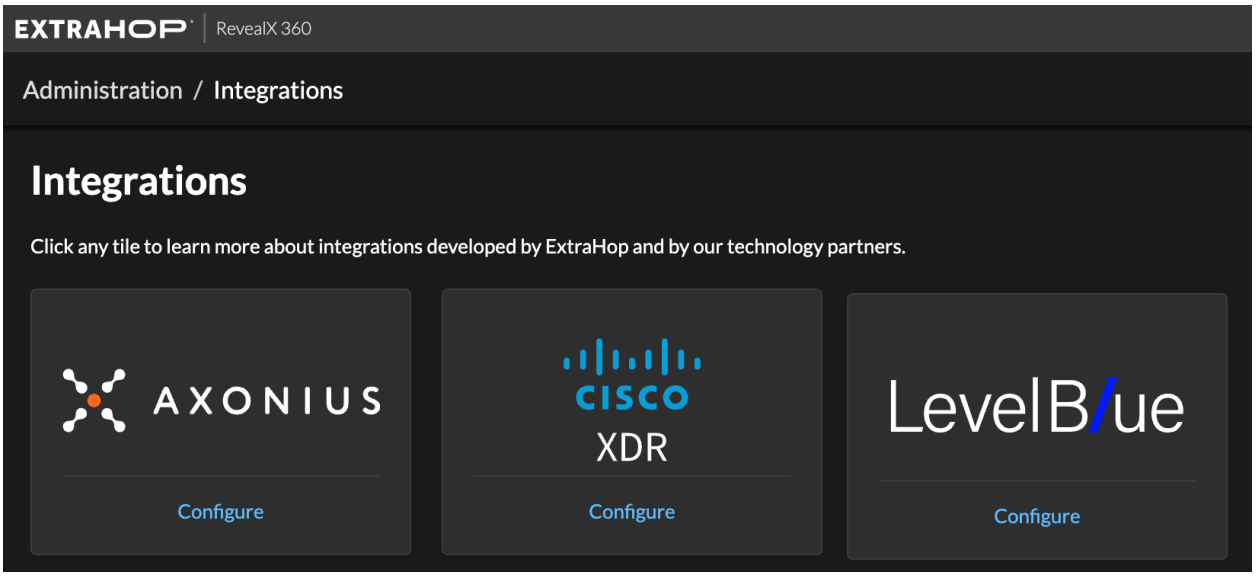
Intégrations ajoutées pour SIEM de nouvelle génération CrowdStrike Falçon et Solution SIEM de sécurité d'entreprise Splunk cet effet de levier règles de notification pour exporter les données de détection ExtraHop vers le SIEM cible.



Intégrations entre LevelBlue, Axonius et Cisco XDR

Les nouvelles intégrations suivantes ont été ajoutées pour vous aider à étudier les données d'équipement et de détection et à y répondre :

- Niveau bleu propose une détection et une réponse gérées (MDR).
- Axonius est un outil de gestion des actifs de cybersécurité.
- Cisco XDR est une solution étendue de détection et de réponse basée sur le cloud.

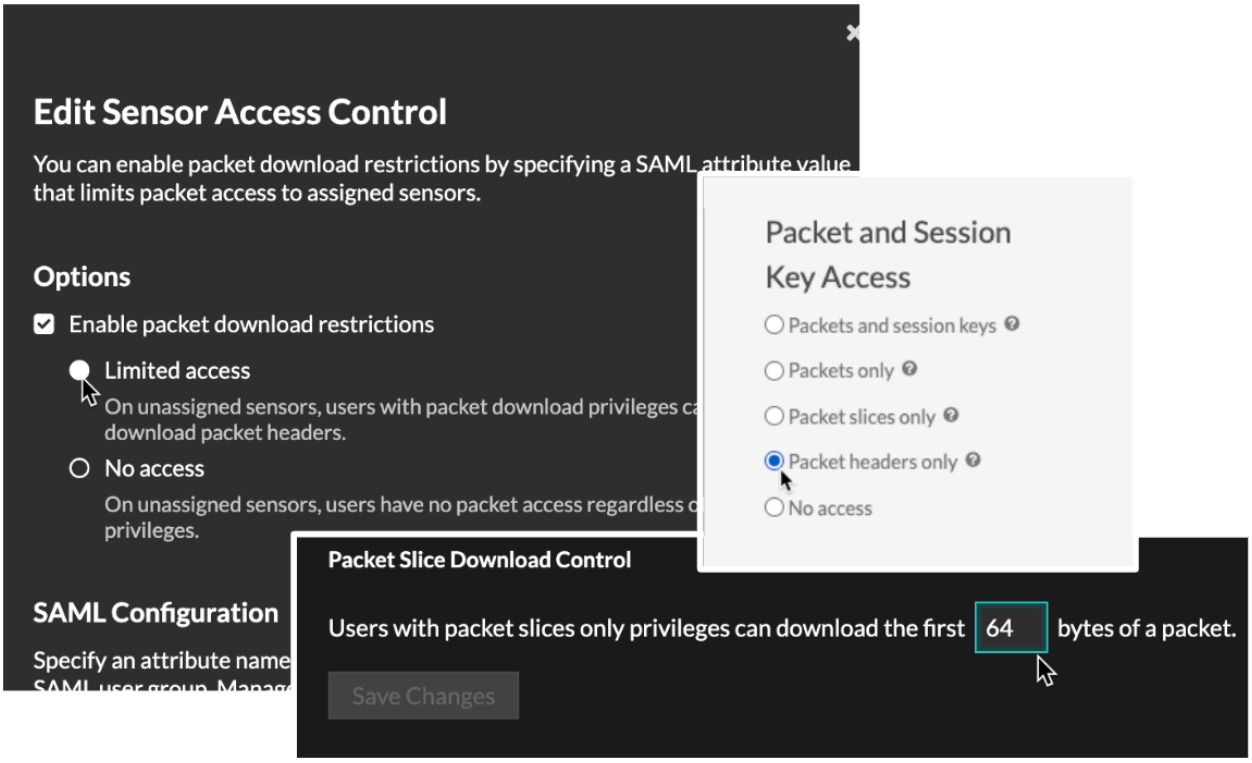


Pour les administrateurs

Contrôle d'accès aux paquets

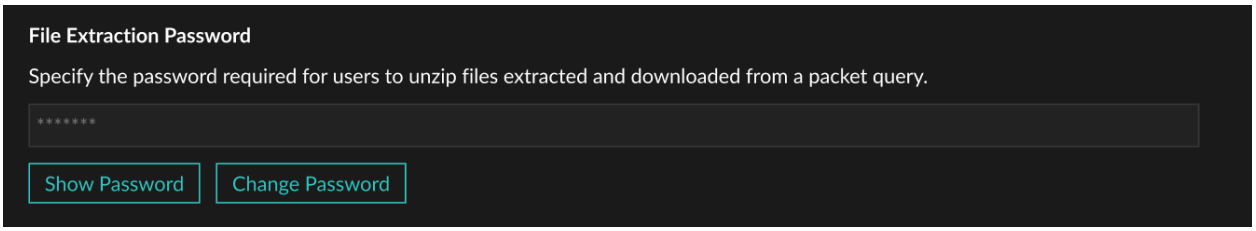
Les administrateurs peuvent désormais accorder privilèges qui permettent aux utilisateurs de télécharger uniquement les en-têtes de paquets. Les administrateurs de RevealX 360 peuvent

également définir politique mondiale pour la taille des tranches de paquet, et activer le contrôle d'accès aux sondes pour accorder l'accès à des groupes d'utilisateurs spécifiques.



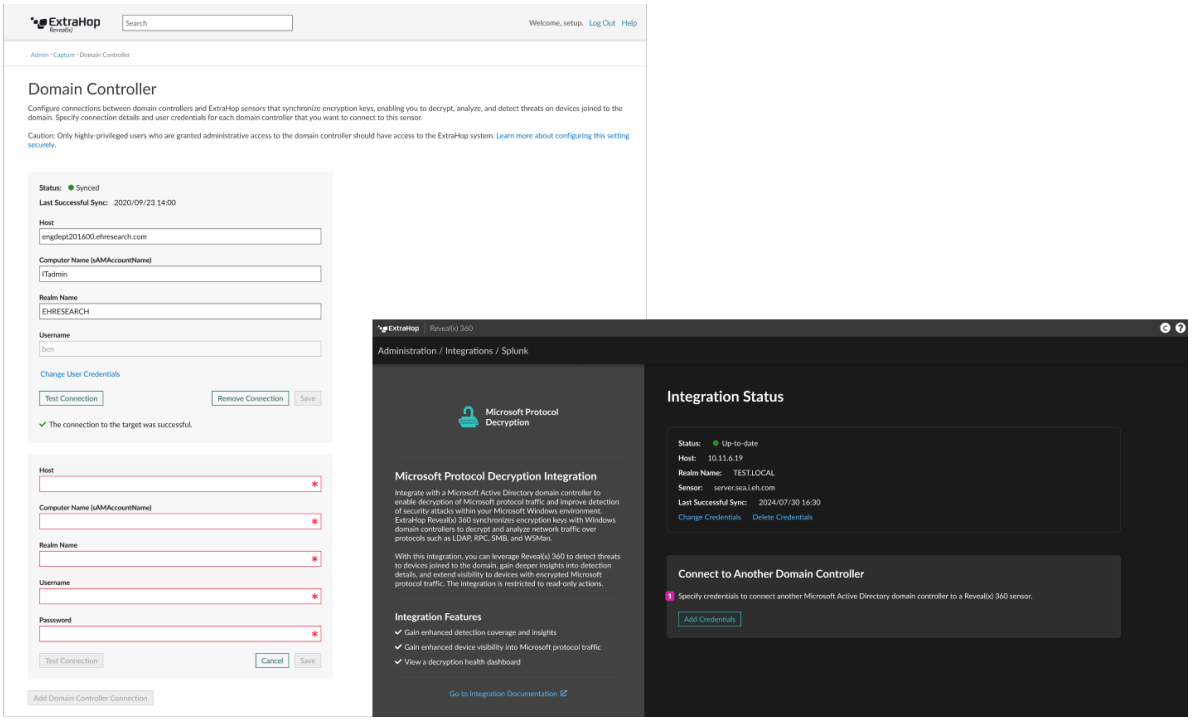
Mot de passe d'extraction de fichiers

Un mot de passe est nécessaire pour ouvrir les fichiers .zip extraits ou gravés à partir de paquets. Les administrateurs peuvent définir le mot de passe d'extraction des fichiers dans les paramètres d'administration de RevealX Enterprise ou RevealX 360 et partagez le mot de passe avec les utilisateurs autorisés.



Décryptage pour plusieurs contrôleurs de domaine

Le système ExtraHop désormais prend en charge la connexion de plusieurs contrôleurs de domaine à une sonde pour déchiffrer le trafic du contrôleur de domaine. Vous pouvez configurer le déchiffrement sur une sonde individuelle sur RevealX Enterprise ou via une intégration sur RevealX 360.



Pour les développeurs d'API

API de déclenchement

Vous pouvez désormais stocker des métriques et accéder aux propriétés du trafic SOCKS et NMF avec le nouveau SOCKS et NMF cours.

API REST

A ajouté le `/appliances/sensortags` point de terminaison du API REST RevealX 360, qui vous permet de visualiser et de gérer les étiquettes des sondes.