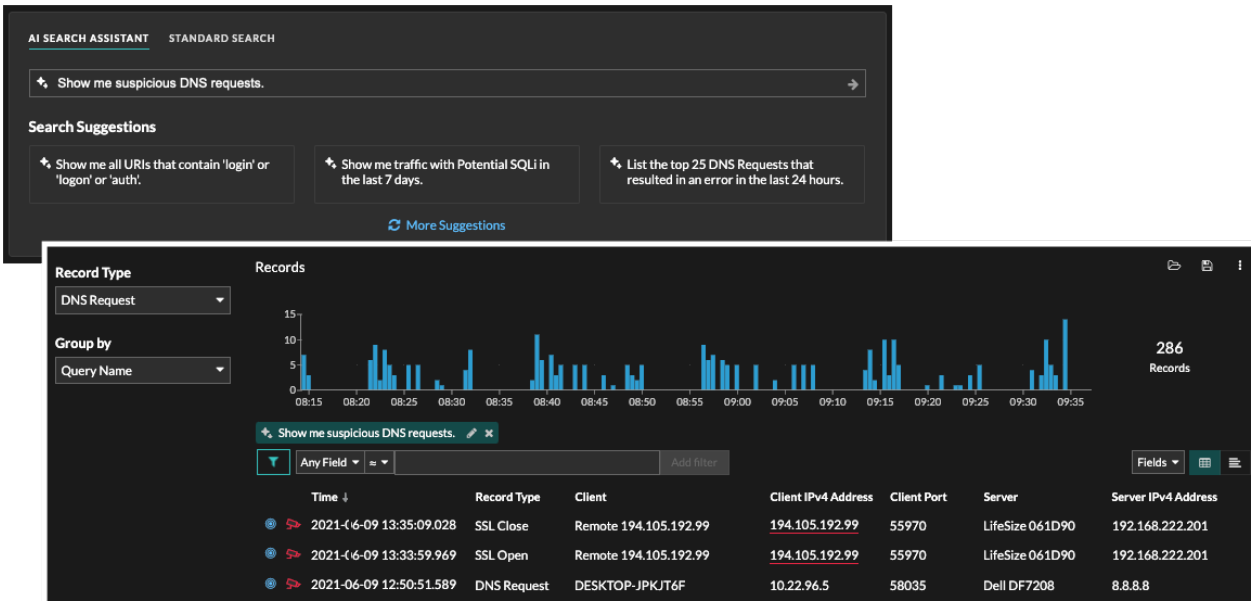
Quoi de neuf

Publié: 2024-07-18

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 9.7.

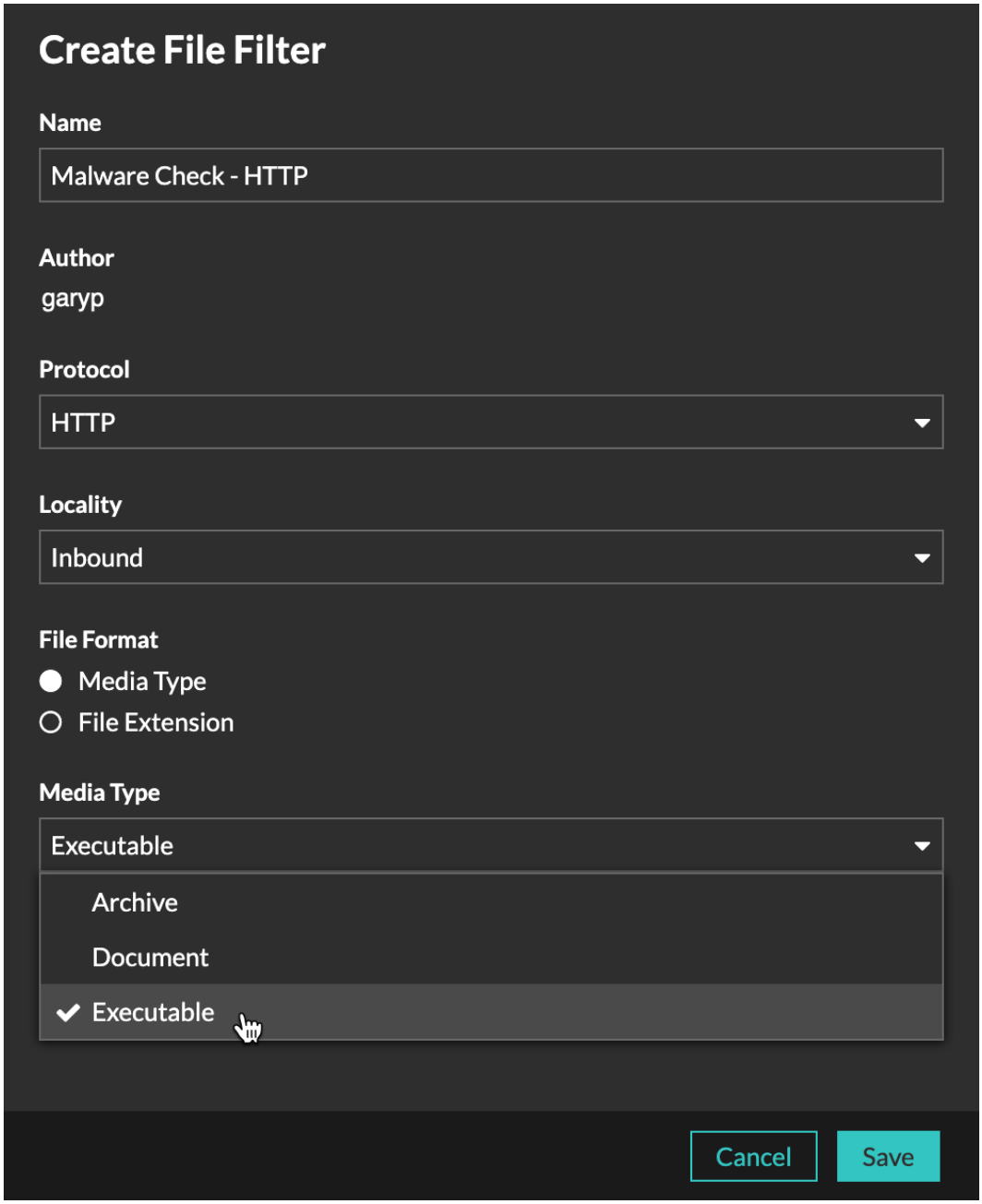
Assistant de recherche IA

Assistant de recherche IA vous permet désormais de lancer des recherches à partir de la page Enregistrements en saisissant une question ou une demande concernant vos enregistrements enregistrés. Cette question, ou invite, est associée à des critères de filtrage et renvoie des résultats de recherche. Les administrateurs de RevealX 360 et RevealX Enterprise doivent activer cette fonctionnalité, qui est désactivée par défaut.



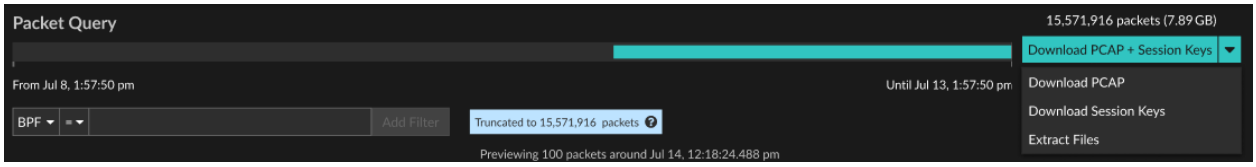
Analyse de fichiers

Tu peux maintenant créer des filtres de fichiers personnalisés qui déterminent quels fichiers sont hachés sur le système à l'aide de l'algorithme de hachage SHA-256. Les hachages de fichiers qui correspondent à une collecte des menaces génèrent une détection, et les données de hachage de fichiers peuvent être interrogées dans des enregistrements.

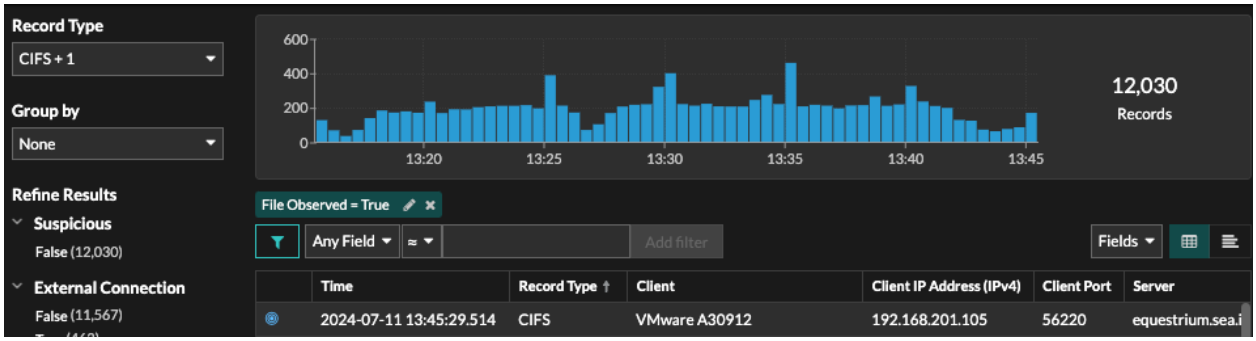


Extraction de fichiers

Tu peux extraire des fichiers à partir de paquets qui contiennent des données provenant du trafic HTTP ou CIFS. Les fichiers extraits sont téléchargés depuis le navigateur sur votre ordinateur local dans un fichier .zip. L'extraction de fichiers (également appelée découpage de fichiers) n'est disponible que pour les utilisateurs ayant accès aux modules NDR et Packet Forensics.

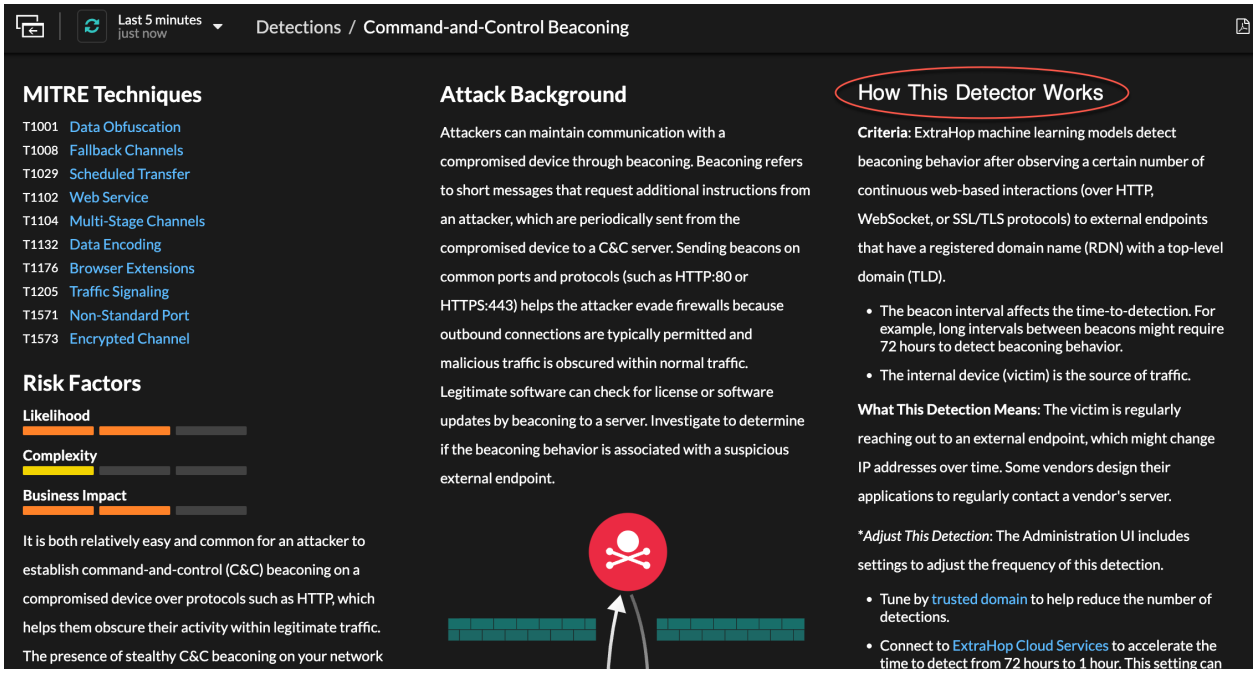


Sur la page Enregistrements, vous pouvez rechercher des types d'enregistrement HTTP ou CIFS et filtrer par « Fichier observé ». Cliquez sur l'icône des paquets à côté de l'enregistrement associé aux fichiers que vous souhaitez extraire.



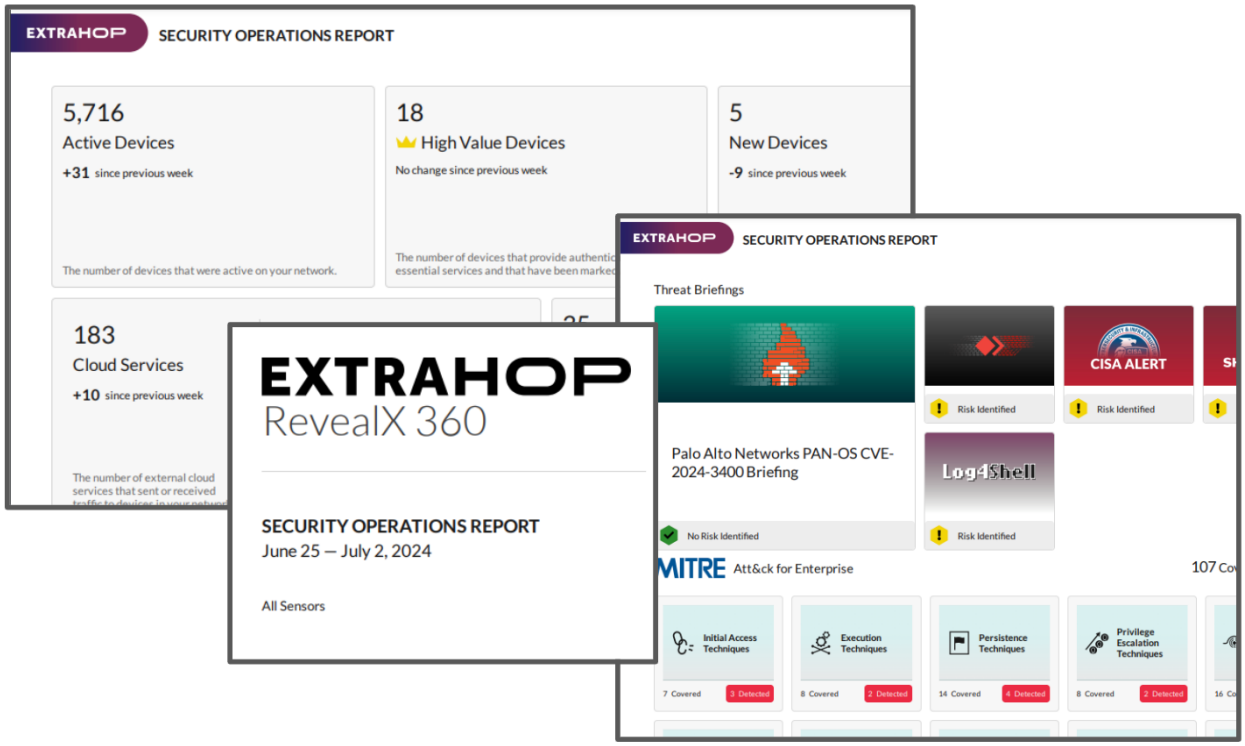
Comment fonctionne ce détecteur

Pour certains types de détection, une section Fonctionnement de ce détecteur est disponible dans détails de détection qui fournit des réponses aux questions fréquemment posées sur les raisons pour lesquelles une détection apparaît dans votre système ExtraHop.



Rapport sur les opérations de sécurité

Le rapport sur les opérations de sécurité (anciennement appelé rapport exécutif) contient un résumé amélioré des indicateurs système importants liés à votre surface d'attaque et à la couverture des menaces.



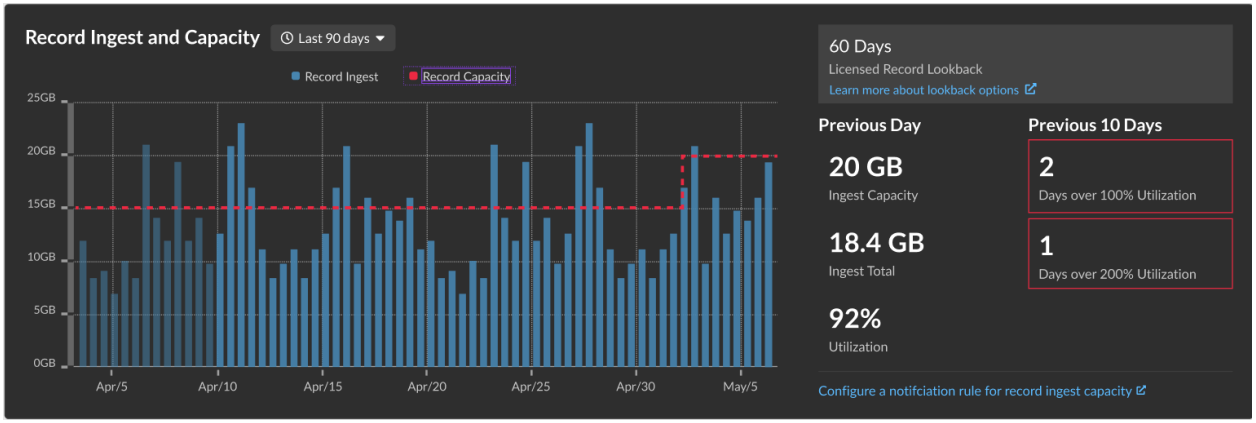
Pour les administrateurs

Nouvelle limite maximale de capteur

Le système ExtraHop peut désormais prendre en charge des consoles qui gèrent jusqu'à 250 capteurs.

Enregistrer les options de rétrospective

À partir du Tableau des records d'ingestion et de capacité, les administrateurs d'ExtraHop pour RevealX 360 peuvent sélectionner un intervalle de 30, 60, 90, 120 ou 180 jours en fonction du nombre d'enregistrements sous licence, qui s'affiche à droite du graphique à barres.



Pour les développeurs d'API

API de déclenchement

Vous pouvez désormais stocker des métriques et accéder aux propriétés du trafic NTP et TFTP avec le nouveau `NTP`La classe `NTP (Network Time Protocol)` vous permet de stocker des métriques et d'accéder à des propriétés sur `NTP_MESSAGE` événements. et `TFTP`La classe `TFTP (Trivial File Transfer Protocol)` vous permet de

`stocker des métriques et d' accéder à des propriétés sur TFTP_REQUEST et TFTP_RESPONSE événements.` cours.

API REST

Tu peux maintenant extraire des fichiers (également connu sous le nom de découpage de fichiers) à partir de paquets via `/packets/search` point de terminaison en spécifiant `output` paramètre comme `extract`.