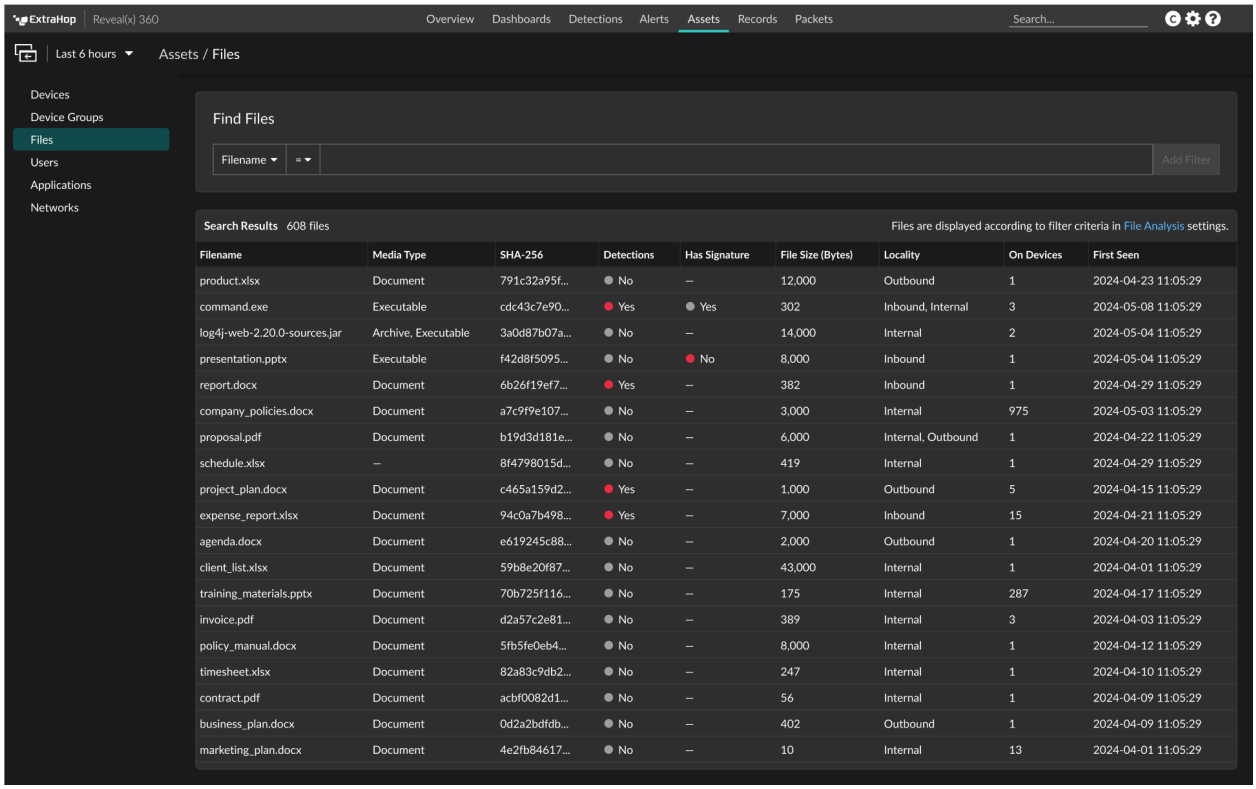
Dossiers

Publié: 2024-10-26

Les métadonnées issues de fichiers hachés constituent un outil précieux pour identifier les programmes malveillants et les risques sur votre réseau. Par exemple, les fichiers téléchargés par plusieurs appareils, les fichiers dont l'extension ne correspond pas au type de support, les fichiers non signés ou les transferts de fichiers sortants ou entrants volumineux sont des observations qui méritent d'être étudiées. La page Fichiers affiche un tableau des fichiers hachés et des informations sur les fichiers associés que vous pouvez filtrer et rechercher. Pour afficher la page Fichiers, cliquez sur **Actifs** dans le menu de navigation supérieur, puis cliquez sur **Dossiers** graphique.

Les fichiers sont hachés à l'aide de l'algorithme de hachage SHA-256 et affichés dans le tableau Fichiers selon les critères de filtrage configurés à partir du Paramètres d'analyse de fichiers. Vous pouvez ajouter des filtres dans Rechercher des fichiers section pour affiner les résultats dans le tableau Fichiers.

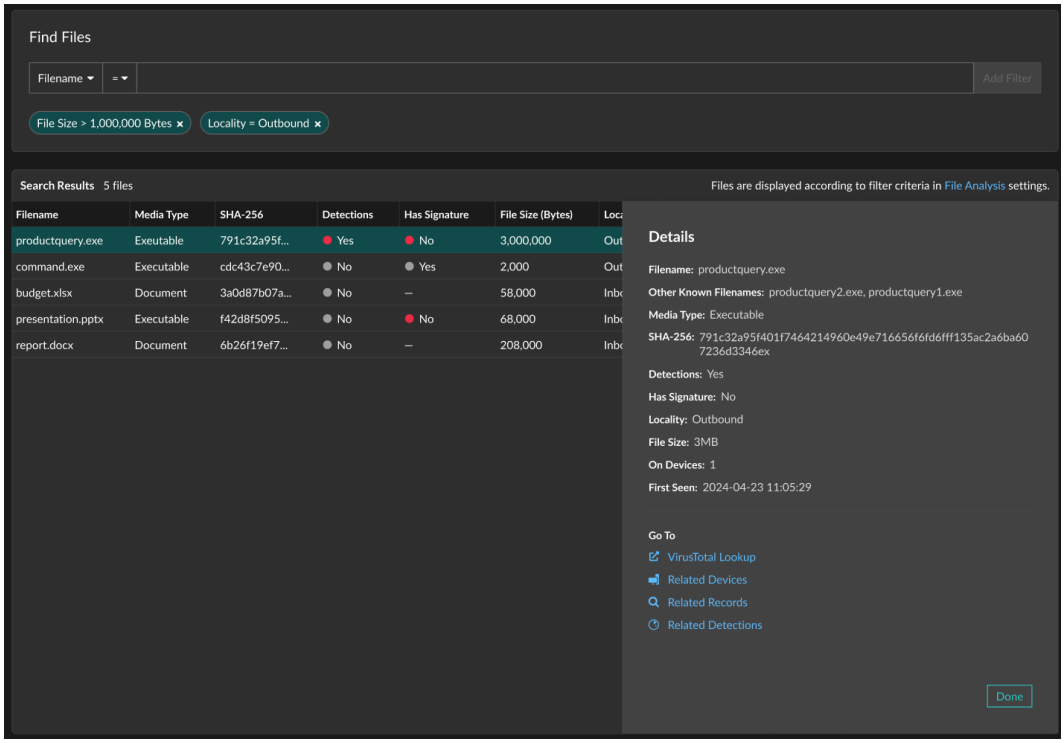


Le tableau Fichiers affiche les informations suivantes pour chaque fichier.

Détail du dossier	Descriptif
Nom de fichier	Le nom du fichier haché. Les autres noms de fichiers renvoyés par le même algorithme de hachage SHA-256 sont affichés dans le volet Détails.
Type de média	Type de support du fichier haché. Les types de fichiers pris en charge sont Document, Archive et Exécutable. Le système ExtraHop détermine le type de support de fichier en analysant les modèles dans l'en-tête et les premiers octets de la charge utile du fichier.

Détail du dossier	Descriptif
SHA-256	Algorithme de hachage de fichier SHA-256 appliqué au fichier. Conseil : vous pouvez trouver des appareils associés à des fichiers hachés spécifiques en ajoutant le filtre SHA-256 à la recherche d'un équipement.
Détections	Indique si le fichier haché a été impliqué dans une détection correspondant à un indicateur d'une collecte des menaces, tel qu'un transfert de fichier malveillant. (Disponible uniquement sur une console connectée à une sonde IDS (Intrusion Detection System) pour les utilisateurs ayant accès au module NDR)
Possède une signature	Indique si une signature a été observée sur le fichier haché, mais ne vérifie pas si la signature est valide.
Taille du fichier	Taille du fichier haché, en octets.
Localité	Localité, ou direction du flux, du fichier haché. Les localités prises en charge sont les suivantes : entrante, sortante et interne.
Sur les appareils	Le nombre d'appareils sur lesquels le fichier haché a été observé.
Vu pour la première fois	L'horodateur auquel le fichier haché a été observé pour la première fois.

Cliquez sur un fichier dans le tableau pour ouvrir le volet Détails et afficher plusieurs liens qui vous permettent d'étudier le hachage du fichier SHA-256.



- Cliquez **Recherche VirusTotal** pour accéder au site VirusTotal et vérifier que le hachage du fichier ne contient pas de contenu malveillant.
- Cliquez **Appareils associés** pour filtrer les appareils en fonction du hachage du fichier et afficher les résultats sur Appareils page.
- Cliquez **Enregistrements associés** pour filtrer les enregistrements en fonction du hachage du fichier et afficher les résultats sur Disques page.
- Cliquez **Détections associées** pour filtrer les détections en fonction du hachage du fichier et afficher les résultats sur Détections page. (Disponible uniquement sur une console connectée à une sonde IDS (Intrusion Detection System) pour les utilisateurs ayant accès au module NDR.)