

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.

Filename	Media Type	SHA-256	Detections	Has Signature	File Size (Bytes)	Locality	On Devices	First Seen
product.xlsx	Document	791c32a95f...	No	—	12,000	Outbound	1	2024-04-23 11:05:29
command.exe	Executable	cdc43c7e90...	Yes	Yes	302	Inbound, Internal	3	2024-05-08 11:05:29
log4j-web-2.20.0-sources.jar	Archive, Executable	3a0d87b07a...	No	—	14,000	Internal	2	2024-05-04 11:05:29
presentation.pptx	Executable	f42d8f5095...	No	No	8,000	Inbound	1	2024-05-04 11:05:29
report.docx	Document	6b26f19ef7...	Yes	—	382	Inbound	1	2024-04-29 11:05:29
company_policies.docx	Document	a7c9f9e107...	No	—	3,000	Internal	975	2024-05-03 11:05:29
proposal.pdf	Document	b19d3d181e...	No	—	6,000	Internal, Outbound	1	2024-04-22 11:05:29
schedule.xlsx	—	8f4798015d...	No	—	419	Internal	1	2024-04-29 11:05:29
project_plan.docx	Document	c465a159d2...	Yes	—	1,000	Outbound	5	2024-04-15 11:05:29
expense_report.xlsx	Document	94c0a7b498...	Yes	—	7,000	Inbound	15	2024-04-21 11:05:29
agenda.docx	Document	e619245c88...	No	—	2,000	Outbound	1	2024-04-20 11:05:29
client_list.xlsx	Document	59b8e20f87...	No	—	43,000	Internal	1	2024-04-01 11:05:29
training_materials.pptx	Document	70b725f116...	No	—	175	Internal	287	2024-04-17 11:05:29
invoice.pdf	Document	d2a57c2e81...	No	—	389	Internal	3	2024-04-03 11:05:29
policy_manual.docx	Document	5fb5fe0eb4...	No	—	8,000	Internal	1	2024-04-12 11:05:29
timesheet.xlsx	Document	82a83c9db2...	No	—	247	Internal	1	2024-04-10 11:05:29
contract.pdf	Document	acb0082d1...	No	—	56	Internal	1	2024-04-09 11:05:29
business_plan.docx	Document	0d2a2bdfdb...	No	—	402	Outbound	1	2024-04-09 11:05:29
marketing_plan.docx	Document	4e2fb84617...	No	—	10	Internal	13	2024-04-01 11:05:29

Le tableau Fichiers affiche les informations suivantes pour chaque fichier.

Détail du dossier

Nom de fichier

Descriptif

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.

The screenshot shows the 'Find Files' interface. At the top, there are search filters: 'File Size > 1,000,000 Bytes' and 'Locality = Outbound'. Below the filters, a table displays search results for 5 files. The first file, 'productquery.exe', is highlighted. To the right of the table, a 'Details' panel provides information for the selected file.

Filename	Media Type	SHA-256	Detections	Has Signature	File Size (Bytes)	Locality
productquery.exe	Executable	791c32a95f...	Yes	No	3,000,000	Outbound
command.exe	Executable	cdc43c7e90...	No	Yes	2,000	Outbound
budget.xlsx	Document	3a0d87b07a...	No	-	58,000	Inbound
presentation.pptx	Executable	f42d8f5095...	No	No	68,000	Inbound
report.docx	Document	6b26f19ef7...	No	-	208,000	Inbound

Details

Filename: productquery.exe
Other Known Filenames: productquery2.exe, productquery1.exe
Media Type: Executable
SHA-256: 791c32a95f401f7464214960e49e716656f6fd6ff135ac2a6ba607236d3346ex
Detections: Yes
Has Signature: No
Locality: Outbound
File Size: 3MB
On Devices: 1
First Seen: 2024-04-23 11:05:29

Go To

- VirusTotal Lookup
- Related Devices
- Related Records
- Related Detections

Done

- 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.)