

Dateien

Veröffentlicht: 2025-02-04

Metadaten aus Hash-Dateien sind ein wertvolles Tool zur Identifizierung von Malware und Risiken in Ihrem Netzwerk. Beispielsweise sind Dateien, die von mehreren Geräten heruntergeladen wurden, Dateien mit einer Erweiterung, die nicht dem Medientyp entspricht, unsignierte Dateien oder große ausgehende oder eingehende Dateiübertragungen Beobachtungen, die es wert sind, untersucht zu werden. Auf der Seite „Dateien“ wird eine Tabelle mit Hash-Dateien und zugehörigen Dateidetails angezeigt, die Sie filtern und durchsuchen können. Um die Seite „Dateien“ anzuzeigen, klicken Sie auf **Vermögenswerte** aus dem oberen Navigationsmenü und klicken Sie dann auf **Dateien** Diagramm.

Dateien werden mit dem SHA-256-Hashing-Algorithmus gehasht und in der Dateitabelle gemäß den Regeln angezeigt, die in der [Einstellungen für die Dateianalyse](#) [🔗](#). Sie können die Ergebnisse in der Tabelle Dateien verfeinern, indem Sie Suchfilterkriterien in der Dateien finden Abschnitt oder indem Sie in der Tabelle auf einen Popup-Operator klicken, um einen Filter hinzuzufügen.

Filename	Media Type	SHA-256	Detections	Is Signed	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	0d2a2bdfb...	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

In der Tabelle Dateien werden die folgenden Details für jede Datei angezeigt.

Detail der Datei

Dateiname

Beschreibung

Der Name der Hash-Datei.

Andere Dateinamen, die von demselben SHA-256-Hashing-Algorithmus zurückgegeben werden, werden im Detailbereich angezeigt.

Art des Mediums

Der Medientyp der Hash-Datei. Unterstützte Dateitypen sind Dokument, Archiv und Ausführbar.

Das ExtraHop-System bestimmt den Datei-Medientyp, indem es Muster im Header und in den Anfangsbytes der Dateinutzlast analysiert.

Detail der Datei	Beschreibung
SHA-256	<p>Der SHA-256-Datei-Hashing-Algorithmus wurde auf die Datei angewendet.</p> <p>Tipp: Du kannst findet Geräte, die bestimmten Hash-Dateien zugeordnet sind indem Sie den SHA-256-Filter zu einer Gerätesuche hinzufügen.</p>
Erkennungen	<p>Gibt an, ob die Hash-Datei an einer Erkennung beteiligt war, die einem Indikator in einer Bedrohungssammlung entsprach, z. B. einer Übertragung böse Datei.</p> <p>(Nur auf einer Konsole verfügbar, die an einen Sensor des Intrusion Detection System (IDS) angeschlossen ist, für Benutzer mit NDR-Modulzugriff)</p>
Ist signiert	Gibt an, ob eine Signatur in der Hash-Datei beobachtet wurde, überprüft aber nicht, ob die Signatur gültig ist.
Größe der Datei	Die Größe der Hash-Datei in Byte.
Lokalität	Die Lokalität oder Flussrichtung der Hash-Datei. Unterstützte Orte sind Inbound, Outbound und Internal.
Auf Geräten	Die Anzahl der Geräte, auf denen die Hash-Datei beobachtet wurde.
Zuerst gesehen	Der Zeitstempel, zu dem die Hash-Datei zum ersten Mal beobachtet wurde.

Klicken Sie auf eine Datei in der Tabelle, um den Detailbereich zu öffnen und mehrere Links anzuzeigen, mit denen Sie den SHA-256-Datei-Hash untersuchen können.

ExtraHop | Reveal(x) 360 | Overview | Dashboards | Detections | Alerts | **Assets** | Records | Packets | Search...

Assets / Files

Find Files

Filename Add Filter

File Size > 500,000 Bytes Locality = Outbound

Search Results 5 files

Filename	Media Type	SHA-256	Detections	Is Signed	File Size (Bytes)	Locality
productquery.exe	Executable	791c32a95f...	Yes	No	3,000,000	Outbound
command.exe	Executable	cdc43c7e90...	No	Yes	1,200,000	Outbound
budget.xlsx	Document	3a0d87b07a...	No	—	580,000	Outbound
presentation.pptx	Executable	f42d8f5095...	No	No	680,000	Outbound
report.docx	Document	6b26f19ef7...	No	—	708,000	Outbound

Files are displayed according to File Analysis rules set by an ExtraHop administrator.

Details

Filename: productquery.exe
 Other Known Filenames: productquery2.exe, productquery1.exe
 Media Type: Executable
 SHA-256: 791c32a95f401f7464214960e49e716656f6fd6fff135ac2a6ba607236d3346ex
 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

- Klicken Sie **VirusTotal-Suche** um zur VirusTotal-Site zu navigieren und den Datei-Hash auf bösartige Inhalte zu überprüfen.
- Klicken Sie **Verwandte Geräte** um Geräte nach dem Datei-Hash zu filtern und Ergebnisse auf der [Geräte](#) Seite.
- Klicken Sie **Verwandte Datensätze** um Datensätze nach dem Datei-Hash zu filtern und Ergebnisse auf der [Aufzeichnungen](#) Seite.
- Klicken Sie **Verwandte Erkennungen** um Erkennungen nach dem Datei-Hash zu filtern und die Ergebnisse auf der [Erkennungen](#) Seite. (Nur auf einer Konsole verfügbar, die an einen IDS-Sensor (Intrusion Detection System) angeschlossen ist, für Benutzer mit Zugriff auf das NDR-Modul.)