

Dateianalyse konfigurieren

Veröffentlicht: 2024-11-03

Mithilfe der Dateianalyse können Sie Dateien angeben, die mit dem SHA-256-Hashing-Algorithmus gehasht werden sollen. Datei-Hashes, die einer Bedrohungssammlung entsprechen, generieren eine Erkennung, und Datei-Hashdaten können in Datensätzen abgefragt werden.

ExtraHop empfiehlt, dass Sie diese Einstellungen über eine ExtraHop-Konsole verwalten. Dies ist die Standardkonfiguration in RevealX 360. Bei RevealX Enterprise verwalten Sensoren diese Einstellungen standardmäßig. Wenn Sie die Einstellungen lieber auf einer Konsole statt auf einem Sensor verwalten möchten, können Sie die Verwaltung auf eine Konsole übertragen.

Voraussetzungen

- Sie benötigen System- und Zugriffsadministration oder Systemadministration (nur RevealX 360) [Benutzerrechte](#).

Konfigurieren Sie eine Größenbeschränkung für Dateifilter

Sie können eine Größenbeschränkung angeben, die global für alle Dateifilter gilt. Jede Datei, die dieses Limit überschreitet, wird nicht gehasht.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen  und klicken Sie dann **Datei-Analyse**.
3. In der Größenbeschränkung (MB) Feld, geben Sie eine Dateigröße in MB an. Der Bereich reicht von 1 bis 1.000.000 MB. Der Standardwert ist 10 MB.
4. Klicken Sie **Speichern**.

Erstellen Sie einen Dateifilter

Sie können benutzerdefinierte Dateifilter erstellen, die bestimmen, welche Dateien auf dem ExtraHop-System gehasht werden. Der ExtraHop Default-Filter wird automatisch aktiviert und so konfiguriert, dass er ausführbare Mediendateien und Dateien hasht, die auf allen Protokollen, Lokalisationen und Dateierweiterungen beobachtet werden, die von der Dateianalyse unterstützt werden. Sie können den Standardfilter deaktivieren, aber Sie können die Filterkonfiguration nicht ändern.



Hinweis Das Aktivieren einer großen Anzahl benutzerdefinierter Dateifilter kann sich auf die Systemleistung auswirken.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen  und klicken Sie dann **Datei-Analyse**.
3. In der Dateifilter Abschnitt, klicken **Filter hinzufügen**.
4. In der Name Feld, geben Sie einen eindeutigen Namen für den Filter ein.
5. Aus dem **Protokoll** Wählen Sie in der Dropdownliste eine der folgenden Protokolloptionen aus:
 - Beliebiges Protokoll (Standard)
 - HTTP
 - SMP
 - FTP

Auswahl **Irgendein Protokoll** hasht nur Dateien, die auf HTTP-, SMB- oder FTP-Protokollen beobachtet wurden.

6. Aus dem **Lokalität** Wählen Sie in der Dropdownliste eine der folgenden Optionen für die Flussrichtung aus:
 - Beliebiger Ort (Standard)
 - Eingehend
 - Intern
 - Ausgehend
7. In der Format der Datei Abschnitt, wählen Sie den Typ der zu filternden Dateien aus:
 - Um nach Medientyp zu filtern, klicken Sie auf **Art des Mediums**, und wählen Sie dann eine der folgenden Medienoptionen aus:
 - Archiv
 - Dokument
 - Ausführbar
 - Um nach Dateierweiterung zu filtern, klicken Sie auf **Dateierweiterung**, und geben Sie dann eine oder mehrere Dateierweiterungen ein, getrennt durch ein Komma. Sie können Erweiterungen in einem der folgenden Formate eingeben: `txt` oder `.txt`.
8. Wählen Sie im Abschnitt Optionen die **Dateifilter aktivieren** Kontrollkästchen, um den Filter zu aktivieren und mit dem Hashing von Dateien zu beginnen, die den Kriterien entsprechen.
9. Optional: Wenn der Dateifilter aktiviert ist, können Sie den **Hash-Dateien in der Tabelle „Dateien“ anzeigen** Kontrollkästchen zur Anzeige von Hash-Dateien und zugehörigen Metadaten in der **Die Tabelle „Dateien“ ist auf der Seite „Assets“ verfügbar** [↗](#).
10. Klicken Sie **Speichern**.

Übertragungsverwaltung von Dateianalyseinstellungen

Für RevealX 360 verwalten ExtraHop-Konsolen standardmäßig die Dateianalyseinstellungen. Für RevealX Enterprise verwalten ExtraHop-Sensoren diese Einstellungen.

Sie können sich an einer Konsole anmelden und die Verwaltung der Dateianalyseinstellungen auf einen Sensor übertragen, oder Sie können sich bei einem Sensor anmelden und die Verwaltung an eine Konsole übertragen.



Hinweis Durch die Übertragung der Verwaltung für diese Einstellungen wird auch die Verwaltung für alle übertragen. **geteilte Einstellungen** [↗](#).

1. Melden Sie sich bei der Konsole oder dem Sensor an, der derzeit die Dateianalyseinstellungen verwaltet, über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Datei-Analyse**.
3. Übertragung der Verwaltung der Dateianalyse auf ein anderes System.

Option	Description
Übertragung vom Sensor zur Konsole	<ol style="list-style-type: none"> 1. klicken Verwaltung von Transfers. 2. Aus dem Konsole verwalten Wählen Sie in der Dropdownliste einen Konsolennamen aus.
Transfer von der Konsole zum Sensor	<ol style="list-style-type: none"> 1. klicken N von N angeschlossene Sensoren. Im Fenster Verwaltungseinstellungen werden eine Liste der Sensoren angezeigt, für die die Konsole gemeinsame Einstellungen verwaltet, und eine Liste der Sensoren, die ihre eigenen Einstellungen verwalten. 2. Klicken Sie auf den Namen des Sensor, dessen Einstellungen Sie selbst verwalten möchten.

Option

Description

3. Loggen Sie sich in den Sensor ein.
4. klicken **Verwaltung von Transfers**.
5. Aus dem **Konsole verwalten** Dropdownliste, wählen **Sensorgerät – Selbst**.