Dateianalyse konfigurieren

Veröffentlicht: 2024-08-09

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 müssen diese Anforderungen erfüllen, um die Dateianalyse auf Ihrem ExtraHop-System anzeigen und konfigurieren zu können.

- Das musst du haben System- und Zugriffsadministrationsrechte.
- Sie müssen Zugriff auf das NDR-Modul haben.
- Ihr ExtraHop-System muss verbunden mit ExtraHop Cloud Services.

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 auf **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 5 MB.
4. Klicken Sie **Speichern**.

Erstellen Sie einen Dateifilter

Sie können benutzerdefinierte Dateifilter erstellen, die bestimmen, welche Dateien auf dem System gehasht werden. Der ExtraHop Default-Filter ist standardmäßig aktiviert. Der Standardfilter kann nicht geändert werden und gilt für ausführbare Medientypdateien, jedes Protokoll, jeden Ort und jede Dateierweiterung.

Hinweis: Das Aktivieren einer großen Anzahl von benutzerdefinierten Dateifiltern kann die Systemleistung beeinträchtigen.

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 auf **Datei-Analyse**.
3. In der Dateifilter Abschnitt, klicken **Filter hinzufügen**.
4. In der Dateifilter erstellen Fenster, in der Name Feld, geben Sie einen eindeutigen Namen ein.
5. Aus dem **Protokoll** Drop-down-Liste, wählen Sie aus den folgenden Optionen:
   - Beliebiges Protokoll (Standard)
   - HTTP
   - CIFS
   - FTP

6. Aus dem **Lokalität** Wählen Sie in der Dropdownliste eine der folgenden Optionen für die Flussrichtung aus:
   - Beliebiger Ort (Standard)
   - Eingehend
   - Intern
   - Ausgehend
7. Für Format der Datei, 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 der Dateierweiterung zu filtern, klicken Sie auf **Datei-Erweiterung**, und geben Sie dann die Dateierweiterungen ein, wobei Sie mehrere Einträge durch ein Komma trennen. Sie können Erweiterungen in einem der folgenden Formate eingeben: `txt` oder `.txt`.
8. Für Optionen, vergewissern Sie sich, dass **Dateifilter aktivieren** Das Kontrollkästchen ist ausgewählt.
9. Klicken Sie **Speichern**.

Übertragungsverwaltung von Dateianalyseeinstellungen

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

Sie können sich an einer Konsole anmelden und die Verwaltung der Dateianalyseeinstellungen 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 Dateianalyseeinstellungen verwaltet, über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann auf **Datei-Analyse**.
3. Übertragung der Verwaltung der Dateianalyse auf ein anderes System.

Option	Description
Übertragung vom Sensor zur Konsole	1. klicken **Verwaltung von Transfers**. 2. Aus dem **Konsole verwalten** Wählen Sie in der Dropdownliste einen Konsolennamen aus.
Transfer von der Konsole zum Sensor	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. 3. Loggen Sie sich in den Sensor ein. 4. klicken **Verwaltung von Transfers**. 5. Aus dem **Konsole verwalten** Dropdownliste, wählen **Sensorgerät — Selbst**.