Dateianalyse konfigurieren

Veröffentlicht: 2025-02-04

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 Dateiregeln

Sie können eine Größenbeschränkung angeben, die global für alle Dateiregeln 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 eine Dateiregel

Sie können benutzerdefinierte Dateiregeln erstellen, die festlegen, welche Dateien auf dem ExtraHop-System gehasht werden. Die ExtraHop-Standardregel wird automatisch aktiviert und so konfiguriert, dass sie ausführbare Mediendateien und Dateien hasht, die auf allen Protokollen, Lokalisationen und Dateierweiterungen beobachtet werden, die von der Dateianalyse unterstützt werden. Sie können die Standardregel deaktivieren, aber Sie können die Regelkonfiguration nicht ändern.

Hinweis: Das Aktivieren einer großen Anzahl benutzerdefinierter Dateiregeln 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 Regeln für Dateien Abschnitt, klicken Sie **Regel hinzufügen**.
4. In der Name Feld, geben Sie einen eindeutigen Namen für die Regel ein.
5. Aus dem **Protokoll** Wählen Sie im Dropdownmenü eine der folgenden Protokolloptionen aus:
   - HTTP
   - SMP
   - FTP
   - Irgendein Protokoll

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

6. Aus dem **Lokalität** Wählen Sie im Dropdownmenü eine der folgenden Optionen für die Flussrichtung aus:
   - Eingehend
   - Intern
   - Ausgehend
   - Beliebiger Ort
7. In der Format der Datei Abschnitt, wählen Sie den Typ der Dateien aus, die gehasht werden sollen:
   - Klicken Sie **Art des Mediums** und wählen Sie dann eine der folgenden Medienoptionen aus:
     - Archivieren
     - Dokument
     - Ausführbar
   - Um nach Dateierweiterung zu hashen, 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 **Dateiregel aktivieren** Kontrollkästchen, um die Regel zu aktivieren und mit dem Hashing von Dateien zu beginnen, die den Kriterien entsprechen.
9. Optional: Wenn die Dateiregel aktiviert ist, können Sie die auswählen **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 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 Einstellungen für die Dateianalyse verwaltet, über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Datei-Analyse**.
3. Übertragen Sie die 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 im Drop-down-Menü 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**.

Option	Description
	5. Aus dem **Konsole verwalten** Drop-down-Menü, wählen **Sensorgerät — Self**.