Laden Sie benutzerdefinierte IDS-Regeln hoch

Veröffentlicht: 2024-08-07

Sie können einen benutzerdefinierten Satz von IDS-Regeln auf ExtraHop IDS-Sensoren hochladen. Das ExtraHop-System konvertiert die Regeln in Erkennungstypen, die Erkennungen generieren, die Sie anzeigen und untersuchen können.

Fügen Sie Regeln, die gemäß den Suricata-Richtlinien formatiert sind, zu einer oder mehreren .rules-Dateien hinzu und laden Sie sie in einer ZIP-Datei hoch. Beim Upload verarbeitet das ExtraHop-System jede Regel. Diese wird in einer Tabelle angezeigt, in der die Signatur-ID, der Name jeder Regel und einer der folgenden Regelstatus angezeigt werden.

• **Akzeptiert:** Das ExtraHop-System hat die Regel erfolgreich verarbeitet.

• **Abgelehnt:** Das ExtraHop-System konnte die Regel nicht verarbeiten. Die Regel enthält möglicherweise einen Formatierungsfehler oder die Regel enthält eine Aktion, ein Protokoll oder eine Option, die derzeit vom ExtraHop-System nicht unterstützt wird. Kontakt ExtraHop-Unterstützung um sich über zukünftige Unterstützung für die Regel zu erkundigen.

• **Upgrade erforderlich:** EIN Eine neuere Version der ExtraHop-Firmware ist erforderlich um die Regel zu unterstützen. Die erforderliche Systemversion wird angezeigt.

Im Folgenden finden Sie einige Überlegungen zu benutzerdefinierten IDS-Regeln:

- Benutzerdefinierte IDS-Regeln müssen als gültig formatiert sein .rules-Datei hochladen.
- Eine oder mehrere Suricata-.rules-Dateien müssen zu einer einzigen ZIP-Datei für den Upload hinzugefügt werden.
- Sie können nicht mehr als 10.000 benutzerdefinierte IDS-Regeln hochladen.
- Durch das Löschen einer Datei werden alle Regeln gelöscht, die mit der hochgeladenen Datei verknüpft sind. Dies kann mehrere Minuten dauern. Benutzern werden möglicherweise weiterhin Erkennungen angezeigt, die auf diesen Regeln basieren, bis der Löschvorgang abgeschlossen ist.
- Durch das Ersetzen einer Datei werden alle Regeln gelöscht, die mit der zuvor hochgeladenen Datei verknüpft sind, und dann werden die Regeln aus der neuen Datei verarbeitet.
- Integrierte IDS-Regeln werden nicht gelöscht oder ersetzt, wenn Sie Ihre benutzerdefinierten IDS-Regeln verwalten. Ihr ExtraHop-System ist mit den ExtraHop Cloud Services verbunden und die neuesten integrierten Regeln werden automatisch auf das System heruntergeladen, sobald aktualisierte Versionen verfügbar sind.

Hinweis: ExtraHop überprüft möglicherweise die hochgeladenen Regeln, um die Genauigkeit der Konvertierung zu überprüfen und um Produktverbesserungen im Hinblick auf die Konvertierung, Richtigkeit und Leistung der Suricata-Regeln anzuleiten.

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 **Benutzerdefinierte IDS-Regeln**.
3. Klicken Sie **Datei hochladen**.
4. Klicken Sie **Wählen Sie eine Datei**, wählen Sie die gewünschte ZIP-Datei aus, und klicken Sie dann auf **Datei hochladen**.
   Der Upload-Vorgang kann mehrere Minuten dauern. Der Dateistatus und die Zeitstempel werden nach Abschluss der Verarbeitung aktualisiert.

Nächste Schritte

Klicken Sie **Erkennungen** von der oberen Navigationsmenüseite aus, um Erkennungen anzuzeigen, die anhand benutzerdefinierter IDS-Regeln generiert wurden. Diese Erkennungen deuten darauf hin, dass die Regel von einer benutzerdefinierten IDS-Datei bereitgestellt wurde und die Signatur-ID der Regel enthält.