Herunterladen von Paketdaten (PCAP-Datei) über die Webbenutzeroberfläche

Inhalt

Einführung

Mithilfe der Webbenutzeroberfläche können Sie die Pakete herunterladen, die die Snort-Regel ausgelöst haben.Der Artikel enthält die Schritte zum Herunterladen von Paketerfassungsdaten (PCAP-Datei) über die Webbenutzeroberfläche eines Sourcefire FireSIGHT-Managementsystems.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der Sourcefire FirePOWER-Geräte und der virtuellen Gerätemodelle verfügen.

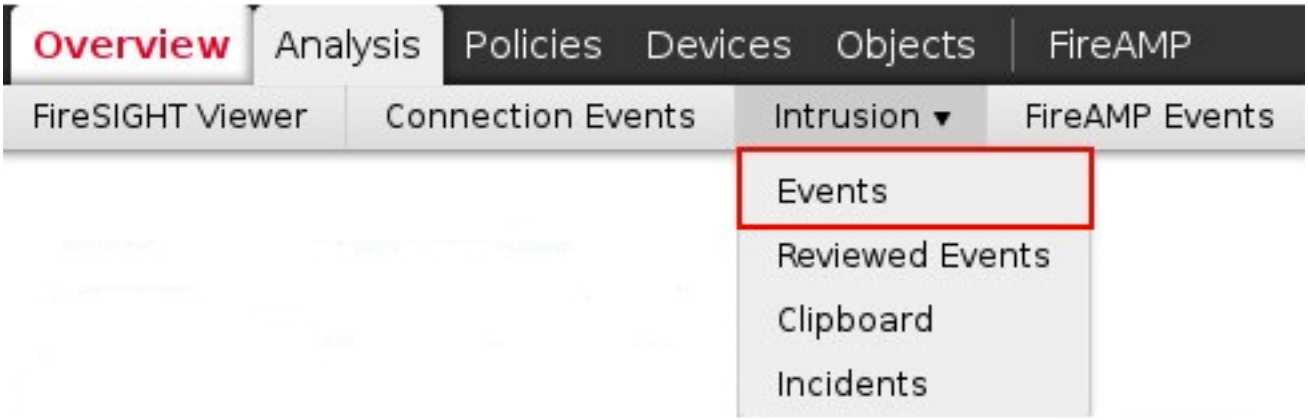
Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Sourcefire FireSIGHT Management Center, auch bekannt als Defense Center, mit Softwareversion 5.2 oder höher.

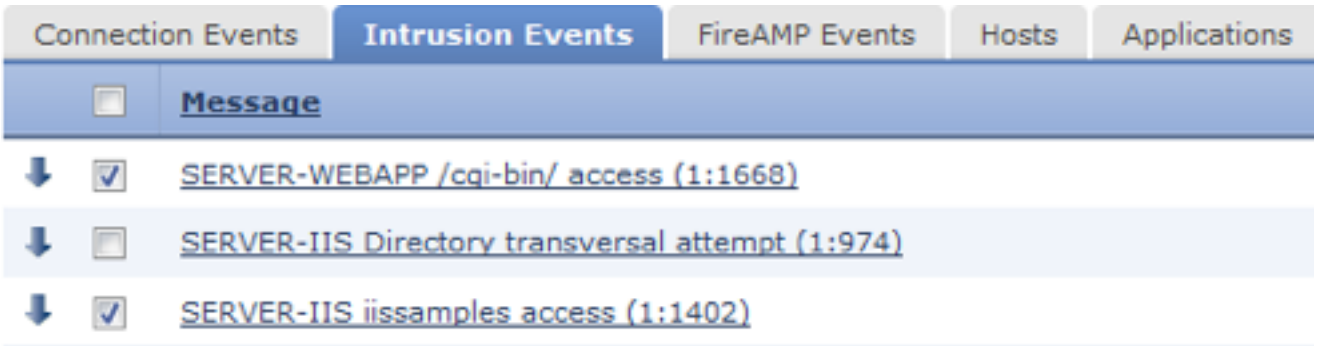
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Schritte zum Herunterladen der PCAP-Datei

Schritt 1: Melden Sie sich bei einem Sourcefire Defense Center oder Management Center an, und navigieren Sie zur Seite "Intrusion Events" (Angriffsversuche) wie folgt:



Schritt 2: Wählen Sie mithilfe des Kontrollkästchens das Ereignis aus, das bzw. die Sie zum Herunterladen von Paketerfassungsdaten (PCAP-Datei) verwenden möchten.



Schritt 3: Navigieren Sie zum Ende der Seite, und wählen Sie:

- Klicken Sie auf Download Packet (Paket herunterladen), um die Pakete herunterzuladen, die das bzw. die ausgewählten Angriffsversuche ausgelöst haben.
- Klicken Sie auf Alle Pakete herunterladen, um alle Pakete herunterzuladen, die die Angriffsversuche in der aktuellen eingeschränkten Ansicht ausgelöst haben.

  Hinweis: Die heruntergeladenen Pakete werden als PCAP gespeichert. Wenn Sie die Paketerfassung analysieren möchten, müssen Sie Software herunterladen und installieren, die eine PCAP-Datei lesen kann.

Schritt 4: Speichern Sie die PCAP-Datei auf Ihrer Festplatte.