Flow-Aufzeichnungen sammeln

Veröffentlicht: 2024-07-17

Sie können automatisch alle Datenflussdatensätze erfassen und speichern, bei denen es sich um Kommunikation auf Netzwerkebene zwischen zwei Geräten über ein IP-Protokoll handelt. Wenn Sie diese Einstellung aktivieren, aber keine IP-Adressen oder Portbereiche hinzufügen, werden alle erkannten Flussdatensätze erfasst. Die Konfiguration von Flow-Datensätzen für die automatische Erfassung ist ziemlich einfach und kann eine gute Möglichkeit sein, die Konnektivität zu Ihrem Recordstore zu testen.

Bevor Sie beginnen
Sie müssen Zugriff auf ein ExtraHop-System haben mit System- und Zugriffsadministrationsrechte.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Automatische Flussaufzeichnungen**.
3. Wählen Sie die **Aktiviert** Ankreuzfeld.
4. In der Intervall veröffentlichen Feld, geben Sie eine Zahl zwischen 60 und 21600 ein.

   Dieser Wert bestimmt, wie oft Datensätze aus einem aktiven Fluss an den Recordstore gesendet werden. Der Standardwert ist 1800 Sekunden.
5. In der IP Adresse Feld, geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich im IPv4-, IPv6- oder CIDR-Format ein.
6. Klicken Sie auf das grüne Plus (**+**) Symbol.

   Sie können einen Eintrag entfernen, indem Sie auf das rote Löschen klicken (**X**) Symbol.
7. In der Portbereiche Feld, geben Sie einen einzelnen Port oder Portbereich ein, und klicken Sie dann auf das grüne Plus (**+**) Symbol.
8. Klicken Sie **Speichern**.

   Flow-Datensätze, die Ihre Kriterien erfüllen, werden jetzt automatisch an Ihren konfigurierten Recordstore gesendet. Warten Sie ein paar Minuten, bis die Aufzeichnungen gesammelt sind.
9. Klicken Sie im ExtraHop-System auf **Rekorde** aus dem Hauptmenü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

   Wenn Sie keine Aufzeichnungen sehen, warten Sie ein paar Minuten und versuchen Sie es erneut. Wenn nach fünf Minuten keine Aufzeichnungen angezeigt werden, überprüfen Sie Ihre Konfiguration oder wenden Sie sich an ExtraHop-Unterstützung.