

Überwachen Sie die Netzwerksegmentierung mit benutzerdefinierten Erkennungen

Veröffentlicht: 2023-09-14

Die Segmentierung Ihres Netzwerk in separate Subnetzwerke kann zur Verbesserung der Sicherheit beitragen, da nur bestimmten Clients der Zugriff auf Server gestattet wird, die vertrauliche Daten enthalten. Durch die Erstellung einer benutzerdefinierten Erkennung können Sie feststellen, wann ein Computer außerhalb eines privilegierten Teilnetzes mit einem Gerät innerhalb des Teilnetzes kommuniziert, sodass Sie sicherstellen können, dass Ihre Sicherheitskonventionen durchgesetzt werden .

In dieser exemplarischen Vorgehensweise erstellen wir eine Gerätegruppe für unser privilegiertes Subnetzwerk und schreiben einen Auslöser, der jedes Mal eine Erkennung auslöst, wenn ein externer Computer die Gruppe kontaktiert.

Erstellen Sie eine Gerätegruppe für das privilegierte Subnetz

Zunächst erstellen wir eine Gerätegruppe, die alle IP-Adressen in den folgenden CIDR-Blöcken enthält:

- 192.168.1,0/24
- 192.168.2,0/24



Hinweis Sie können diese CIDR-Blöcke so ändern, dass sie einem bestimmten Subnetz in Ihrer Umgebung entsprechen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**.
3. klicken **Gerätegruppen**.
4. klicken **Gerätegruppe erstellen**.
5. In der Name der Gruppe Textfeld, Typ `Privileged Network`.
6. klicken **Dynamisch**.
7. klicken **Alle abgleichen** und wählen Sie dann **Beliebiges abgleichen** aus dem Drop-down-Menü.
8. klicken **Name**, und wählen Sie dann **IP-Adresse** aus dem Drop-down-Menü.
9. Geben Sie in das Textfeld `192.168.1.0/24`.
10. klicken **Filter hinzufügen** um einen zusätzlichen Filter hinzuzufügen.
11. klicken **Name**, und wählen Sie dann **IP-Adresse** aus dem Drop-down-Menü.
12. Geben Sie in das Textfeld `192.168.2.0/24`.


Erstellen Sie einen Auslöser, um benutzerdefinierte Erkennungen zu generieren

Als Nächstes erstellen wir den Auslöser, der benutzerdefinierte Erkennungen generiert. Trigger generieren benutzerdefinierte Erkennungen, indem sie den aufrufen `commitDetection` Funktion im Trigger-Skript.

Der Auslöser identifiziert Datenverkehr von außerhalb des privilegierten Subnetzes, indem er die `hasTrigger` Eigenschaft des Client-Geräts für jeden Fluss. Die `hasTrigger` Diese Eigenschaft gibt an, ob der Auslöser auf dem Gerät ausgeführt wird. Da der Auslöser allen Geräten in der Gerätegruppe Privilegiertes Netzwerk zugewiesen ist, `hasTrigger` Die Eigenschaft wird für alle Geräte außerhalb des Subnetzes auf `False` gesetzt.



Hinweis Weitere Informationen zur `CommitDetection`-Funktion finden Sie in der [Trigger-API-Referenz](#).

1. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Auslöser**.
2. klicken **Erstellen**.
3. In der Name Feld, Typ `Network Segmentation Custom Detection`.
4. In der Beschreibung Feld, geben Sie den folgenden Text ein:

```
Creates a detection every time a device in the privileged network communicates with a device outside of the privileged network.
```


5. Klicken Sie in den Ereignisse Feld und Auswahl **FLOW_CLASSIFY**.
Der Auslöser wird für das FLOW_CLASSIFY-Ereignis ausgeführt, das ausgeführt wird, wenn ein Flow anfänglich einem bestimmten Protokoll zugeordnet ist. Dieser Schritt stellt sicher, dass alle Datenflüsse auf verdächtiges Verhalten untersucht werden.
6. In der Zuweisungen Feld, Typ `Privileged Network`, und wählen Sie dann die Gruppe aus, die Sie im vorherigen Verfahren erstellt haben.
7. Geben Sie im rechten Bereich das folgende Triggerskript ein:

```
const client = Flow.client.device;
const server = Flow.server.device;
if (!client.hasTrigger) {
  commitDetection('network_segmentation_breach', {
    title: 'Network Segmentation Breach',
    description: `Device ${client.id} accessed privileged device ${server.id} over ${Flow.l7proto}`,
    categories: ['sec.caution'],
    riskScore: 80,
    participants: [{
      object: client,
      role: 'offender'
    }, {
      object: server,
      role: 'victim'
    }],
    identityKey: [client.id, server.id].join('!!!'),
  });
}
```

8. klicken **Speichern** und dann klicken **Erledigt**.

Erstellen Sie einen benutzerdefinierten Erkennungstyp


Als Nächstes erstellen wir einen benutzerdefinierten Erkennungstyp, mit dem Sie benutzerdefinierten Erkennungen Anzeigenamen und MITRE-Kategorien hinzufügen können.

1. Klicken Sie auf das Symbol Systemeinstellungen  und dann klicken **Erkennungskatalog**.
2. klicken **Erstellen**.
3. In der Name anzeigen Feld, Typ `Network Segmentation Breach`.
4. In der Erkennungstyp-ID Feld, Typ `network_segmentation_breach`.
5. klicken **Speichern**.

Benutzerdefinierte Erkennungen anzeigen

Nachdem Sie den Auslöser gespeichert haben, können Sie die vom Auslöser generierten Erkennungen auf der Seite Erkennungen anzeigen.

1. klicken **Erkennungen**.

2. klicken **Typen**.
3. klicken **Verletzung der Netzwerksegmentierung** um Details zu jeder einzelnen Erkennung anzuzeigen.
 -  **Hinweis** **Verletzung der Netzwerksegmentierung** erscheint nur, wenn der Auslöser während des ausgewählten Zeitintervalls Erkennungen generiert.

Nächste Schritte

- [Eine Benachrichtigungsregel erstellen](#) um E-Mails über Entdeckungen zu versenden, die bestimmten Kriterien entsprechen.