Monitor network segmentation with custom detections

Published: 2024-04-02

Segmenting your network into discrete subnetworks can help improve security by only allowing certain clients to access servers that contain sensitive data. By creating a custom detection, you can identify when a machine outside of a privileged subnetwork communicates with a device inside of the subnetwork, so you can ensure that your security conventions are being enforced.

In this walkthrough, we'll create a device group for our privileged subnetwork and write a trigger that creates a detection every time an outside machine contacts the group.

Create a device group for the privileged subnetwork

First, we'll create a device group that contains all IP addresses in the following CIDR blocks:

- 192.168.1.0/24
- 192.168.2.0/24

Note: You can modify these CIDR blocks to match a specific subnetwork in your environment.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click **Assets**.
3. Click **Device Groups**.
4. Click **Create Device Group**.
5. In the Group Name text box, type `Privileged Network`.
6. Click **Dynamic**.
7. Click **Match All** and then select **Match Any** from the drop-down menu.
8. Click **Name**, and then select **IP Address** from the drop-down menu.
9. In the text box, type `192.168.1.0/24`.
10. Click **Add Filter** to add an additional filter.
11. Click **Name**, and then select **IP Address** from the drop-down menu.
12. In the text box, type `192.168.2.0/24`.

Create a trigger to generate custom detections

Next, we will create the trigger that generates custom detections. Triggers generate custom detections by calling the `commitDetection` function in the trigger script.

The trigger identifies traffic from outside the privileged subnetwork by checking the `hasTrigger` property of the client device for each flow. The `hasTrigger` property indicates whether the trigger is running on the device. Because the trigger is assigned to all devices in the Privileged Network device group, the `hasTrigger` property will be false for all devices outside of the subnetwork.

Note: For more information about the commitDetection function, see the Trigger API Reference.

1. Click the System Settings icon and then click **Triggers**.
2. Click **Create**.
3. In the Name field, type `Network Segmentation Custom Detection`.

4. In the Description field, type the following text:

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

5. Click in the Events field and select **FLOW_CLASSIFY**.

   The trigger runs on the FLOW_CLASSIFY event, which runs as a flow is initially associated with a specific protocol. This step ensures that all flows are investigated for suspicious behavior.

6. In the Assignments field, type `Privileged Network`, and then select the group you created in the previous procedure.
7. In the right pane, type the following trigger script:

```
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. Click **Save** and then click **Done**.

Create a custom detection type

Next, we will create a custom detection type, which enables you to add display names and MITRE categories to custom detections.

1. Click the System Settings icon and then click **Detection Catalog**.
2. Click **Create**.
3. In the Display Name field, type `Network Segmentation Breach`.
4. In the Detection Type ID field, type `network_segmentation_breach`.
5. Click **Save**.

View custom detections

After you save the trigger, you can view detections the trigger generates on the Detections page.

1. Click **Detections**.
2. Click **Types**.
3. Click **Network Segmentation Breach** to view details about each individual detection.

   Note: **Network Segmentation Breach** only appears if detections are generated by the trigger during the selected time interval.

Next steps

- Create a notification rule to send emails about detections that match specific criteria.