Surveillez la segmentation du réseau à l'aide de détections personnalisées

Publié: 2024-08-08

La segmentation de votre réseau en sous-réseaux discrets peut contribuer à améliorer la sécurité en autorisant uniquement certains clients à accéder aux serveurs contenant des données sensibles. En créant une détection personnalisée, vous pouvez identifier le moment où une machine située en dehors d'un sous-réseau privilégié communique avec un équipement à l'intérieur du sous-réseau, afin de vous assurer que vos conventions de sécurité sont appliquées.

Dans cette procédure pas à pas, nous allons créer un groupe d'équipements pour notre sous-réseau privilégié et écrire un déclencheur qui crée une détection chaque fois qu'une machine extérieure contacte le groupe.

Création d'un groupe déquipements pour le sous-réseau privilégié

Nous allons d'abord créer un groupe déquipements contenant toutes les adresses IP des blocs CIDR suivants :

- 192,168.1,0/24
- 192,168.2,0/24

Note: Vous pouvez modifier ces blocs CIDR pour qu'ils correspondent à un sous-réseau spécifique de votre environnement.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Actifs**.
3. Cliquez **Groupes d'appareils**.
4. Cliquez **Créer un groupe d'appareils**.
5. Dans le Nom du groupe zone de texte, tapez `Privileged Network`.
6. Cliquez **Dynamique**.
7. Cliquez **Tout faire correspondre** puis sélectionnez **Faites correspondre n'importe lequel** depuis le menu déroulant.
8. Cliquez **Nom**, puis sélectionnez **Adresse IP** depuis le menu déroulant.
9. Dans la zone de texte, tapez `192.168.1.0/24`.
10. Cliquez **Ajouter un filtre** pour ajouter un filtre supplémentaire.
11. Cliquez **Nom**, puis sélectionnez **Adresse IP** depuis le menu déroulant.
12. Dans la zone de texte, tapez `192.168.2.0/24`.

Créez un déclencheur pour générer des détections personnalisées

Ensuite, nous allons créer le déclencheur qui génère des détections personnalisées. Les déclencheurs génèrent des détections personnalisées en appelant le `commitDetection` fonction dans le script du déclencheur.

Le déclencheur identifie le trafic provenant de l'extérieur du sous-réseau privilégié en cochant la `hasTrigger` propriété de l'équipement client pour chaque flux. Le `hasTrigger` Cette propriété indique si le déclencheur est en cours d'exécution sur l'équipement. Comme le déclencheur est attribué à tous les appareils du groupe d'équipements Privileged Network, `hasTrigger` cette propriété sera fausse pour tous les appareils situés en dehors du sous-réseau.

Note: Pour plus d'informations sur la fonction CommitDetection, consultez le Référence de l'API Trigger.

1. Cliquez sur l'icône des paramètres système puis cliquez sur **DÉCLENCHEURS**.
2. Cliquez **Créez**.
3. Dans le Nom champ, type `Network Segmentation Custom Detection`.
4. Dans le Descriptif dans ce champ, saisissez le texte suivant :

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

5. Cliquez dans le Évènements champ et sélectionnez **FLOW_CLASSIFY**.

   Le déclencheur s'exécute sur l'événement FLOW_CLASSIFY, qui s'exécute lorsqu'un flux est initialement associé à un protocole spécifique. Cette étape garantit que tous les flux sont examinés pour détecter tout comportement suspect.
6. Dans le Missions champ, type `Privileged Network`, puis sélectionnez le groupe que vous avez créé lors de la procédure précédente.
7. Dans le volet droit, tapez le script déclencheur suivant :

```
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. Cliquez **Enregistrer** puis cliquez sur **Terminé**.

Création d'un type de détection personnalisé

Nous allons ensuite créer un type de détection personnalisé, qui vous permet d'ajouter des noms d'affichage et des catégories MITRE aux détections personnalisées.

1. Cliquez sur l'icône des paramètres système puis cliquez sur **Catalogue de détection**.
2. Cliquez **Créez**.
3. Dans le Nom d'affichage champ, type `Network Segmentation Breach`.
4. Dans le ID du type de détection champ, type `network_segmentation_breach`.
5. Cliquez **Enregistrer**.

Afficher les détections personnalisées

Après avoir enregistré le déclencheur, vous pouvez consulter les détections générées par le déclencheur sur la page Détections.

1. Cliquez **Détections**.
2. Cliquez **Les types**.
3. Cliquez **Violation de segmentation du réseau** pour afficher les détails de chaque détection individuelle.

Note: **Violation de segmentation du réseau** apparaît uniquement si des détections sont générées par le déclencheur pendant l'intervalle de temps sélectionné.

Prochaines étapes

- Création d'une règle de notification pour envoyer des e-mails concernant les détections répondant à des critères spécifiques.