Commettre un enregistrement personnalisé pour surveiller les activités portuaires suspectes

Publié: 2024-01-31

La plateforme ExtraHop peut vous aider à gagner en visibilité et à accéder en temps réel aux premiers indicateurs d'attaque sur votre réseau. L'une des mesures de sécurité proactives que vous pouvez prendre consiste à surveiller les ports que vous considérez comme vulnérables aux chevaux de Troie et autres programmes malveillants.

Par exemple, 12345 étant une séquence facile à mémoriser, ce numéro est souvent sélectionné lors de la configuration d'un numéro de port par défaut pour un serveur ou un programme, faisant de cette valeur de port une cible populaire auprès des attaquants.

Dans cette procédure pas à pas, vous allez écrire un déclencheur qui valide chaque transaction dépassant une valeur de port suspecte dans un enregistrement, puis vous allez créer une requête pour consulter les enregistrements collectés.

Prérequis

- Vous devez avoir accès à un système ExtraHop avec un compte utilisateur doté de privilèges d' administration du système et des accès.
- Votre système ExtraHop doit être connecté à un espace de stockage des enregistrements.
- Votre réseau doit être configuré pour autoriser le trafic via le port 12345.
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant le Disques et déclencheurs.
- Familiarisez-vous avec les processus de création de déclencheurs en remplissant le Procédure pas à pas du déclencheur.

Écrivez le déclencheur

Dans les étapes suivantes, vous allez écrire un déclencheur qui recherche le trafic du serveur sur le port 12345, puis qui valide un enregistrement personnalisé de chaque transaction dans un espace de stockage des enregistrements.

1. Connectez-vous à un système ExtraHop connecté à un espace de stockage des enregistrements.
2. Cliquez sur l'icône des paramètres système, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le Nom champ, type `Activité portuaire suspecte`.
5. Dans le Évènements champ, sélectionnez **FLOW_CLASSIFY**.
6. Dans le volet droit, ajoutez le code déclencheur suivant à l'éditeur :

```
if (Flow.server && Flow.server.port === 12345) {
    commitRecord('Trojan', {
        description: 'Possible NetBus or other trojan',
        protocol:Flow.l7proto
    });
}
```

Pour capturer toutes les transactions sur le port, le déclencheur invoque la classe Flow. Le déclencheur indique « Trojan » comme type d'enregistrement et ajoute deux propriétés au contenu de l'enregistrement : une description et le protocole de la transaction, s'il est connu.

7. Cliquez **Enregistrer**.
8. Cliquez **Afficher les options avancées** puis sélectionnez **Attribuer à tous les appareils**.

   Important: Lorsque vous créez vos propres déclencheurs, attribuez des déclencheurs uniquement aux appareils spécifiques à partir desquels vous devez collecter des métriques afin de minimiser l'impact de vos déclencheurs sur les performances du système ExtraHop.
9. Cliquez **Enregistrer et fermer**, puis laissez le déclencheur fonctionner pendant au moins dix minutes.

Interrogez et visualisez les enregistrements personnalisés

Au cours des étapes suivantes, vous allez rechercher les enregistrements personnalisés enregistrés dans l'espace de stockage des enregistrements et créer une requête d'enregistrement enregistrée en fonction des critères de recherche.

1. Dans la navigation de haut niveau, cliquez sur **Enregistrements**.
2. À partir du **Tout type d'enregistrement** menu déroulant, sélectionnez **Trojan**.
3. Cliquez **Afficher les enregistrements**.
4. À partir du **Champs** menu déroulant, sélectionnez **Tout sélectionner**.
5. Cliquez sur **Vue verbeuse** icône.
   Le volet de contenu affiche les champs d'enregistrement personnalisés. Outre les champs de description et de protocole spécifiés dans le déclencheur, l'enregistrement inclut les propriétés suivantes :
   - ID de flux
   - client
   - Adresse du client
   - Port du client
   - serveur
   - Adresse du serveur
   - Port du serveur
6. Cliquez sur **Enregistrer** icône en haut à droite de la page.
7. Dans le Nom champ, type `Trojans possibles`, puis cliquez **Enregistrer**.

Vérifiez les enregistrements pour détecter les indicateurs de programme malveillant

Si votre système est touché par une attaque de programme malveillant ou si vous découvrez qu'un nouveau programme malveillant circule, vous pouvez vérifier dans vos dossiers si votre système a été ciblé.

Par exemple, si vous apprenez qu'un nouveau cheval de Troie est souvent envoyé via le port 12345, vous pouvez ouvrir la requête Possible Trojans enregistrée ci-dessus et vérifier l'activité suivante :

- Transactions effectuées via des protocoles inattendus. Par exemple, vous pouvez vous attendre à voir du trafic IMAP sur le port 12345, mais pas du trafic SSH.
- Transactions effectuées via des protocoles non classifiés, qui sont affichées dans les résultats de la requête sous la forme tcp:12345. Les protocoles non classifiés ne sont pas reconnus par le système ExtraHop et peuvent être suspects.

- Adresses IP des clients associées à des transactions effectuées via des protocoles inattendus ou non classifiés, et si l'adresse IP provient d'un environnement local non fiable.
- Horodatage des transactions que vous trouvez douteuses et qui ont eu lieu en dehors des heures de bureau.

Le fait de limiter les transactions suspectes vous permet de déterminer si vous êtes confronté à un problème lié à un programme malveillant afin de pouvoir commencer à le résoudre.