

Collectez des records L7 à l'aide d'un déclencheur

Publié: 2024-11-04


Les protocoles L7 peuvent être validés (collectés et stockés) sous forme d'enregistrement via une fonction de déclencheur globale. Les enregistrements L7 incluent les messages, les transactions et les sessions envoyés via les protocoles L7 courants tels que DNS, HTTP et TLS.

Dans les étapes suivantes, vous allez apprendre à collecter des enregistrements pour tout équipement qui envoie ou reçoit une Réponse HTTP.

En savoir plus sur [Enregistrements ExtraHop](#).

Tout d'abord, nous allons écrire un déclencheur pour collecter des informations à partir du type d'enregistrement HTTP intégré avec la méthode `commitRecord()`, qui est disponible sur tous [classes de protocoles](#). La syntaxe de base du déclencheur est `<protocol>.commitRecord()`. Ensuite, nous attribuerons le déclencheur à un serveur Web. Enfin, nous vérifierons que les enregistrements sont envoyés à l'espace de stockage des enregistrements.

Avant de commencer

- Vous devez disposer d'un espace de stockage des enregistrements configuré, tel qu'un [espace de stockage des enregistrements ExtraHop](#), [Splunk](#), ou [Google BigQuery](#).
 - Ces instructions supposent une certaine familiarité avec [Déclencheurs ExtraHop](#), qui nécessitent de l'expérience avec JavaScript. Alternativement, vous pouvez [configurer la collection d'enregistrements L7](#) via le système ExtraHop.
1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
 2. Cliquez sur l'icône Paramètres système , puis cliquez sur **éléments déclencheurs**.
 3. Cliquez **Créer**.
 4. Dans le Créer un déclencheur volet, complétez vos informations, comme dans l'exemple suivant :
 - **Nom:** Réponses HTTP
 - **Descriptif:** Ce déclencheur collecte les réponses HTTP.
 5. Cochez la case à côté de **activer le journal de débogage**.
 6. Dans la liste déroulante Événements, sélectionnez **HTTP_RESPONSE**.
 7. Dans le **Devoirs** zone de texte, recherchez un serveur Web actif pour lequel vous souhaitez collecter des enregistrements et sélectionnez le serveur.
 8. Dans le volet droit, saisissez l'exemple de code suivant :

```
HTTP.commitRecord();
debug ("committing HTTP responses");
```

Ce code génère des enregistrements pour le type d'enregistrement HTTP lorsque `HTTP_RESPONSE` l'événement se produit et correspond au format d'enregistrement intégré pour HTTP.

9. Cliquez **Enregistrer**.

Prochaines étapes

Attendez quelques minutes que les enregistrements soient collectés, puis vérifiez que vos enregistrements sont collectés à l'étape suivante en cliquant sur **Disques** dans le menu supérieur, puis cliquez sur **Afficher les enregistrements** pour lancer une requête.

Si aucun enregistrement HTTP ne s'affiche au bout de 5 minutes, cliquez sur **Journal de débogage** onglet en bas de la page dans l'éditeur de déclencheurs pour voir s'il existe des erreurs que vous pouvez résoudre. Si le déclencheur est en cours d'exécution, le message « validation des réponses HTTP » s'affiche. Si aucun enregistrement n'apparaît après l'exécution du déclencheur, contactez [Assistance ExtraHop](#).