

Requête d'enregistrements via l'API REST

Publié: 2024-09-26

L'API REST ExtraHop vous permet de rechercher des enregistrements stockés sur un espace de stockage des enregistrements. En interrogeant des enregistrements à l'aide d'un script d'API REST, vous pouvez importer des enregistrements dans une application tierce, telle que Microsoft Excel. En outre, si votre requête correspond à un nombre d'enregistrements supérieur au nombre maximal d'enregistrements renvoyés par l'API REST, vous pouvez configurer le script pour qu'il recherche de manière récursive les enregistrements restants. Dans cette rubrique, nous présentons des méthodes permettant d'interroger des enregistrements via l'explorateur d'API REST ExtraHop et un script Python.

Avant de commencer

- Vous devez vous connecter au sonde ou console avec un compte disposant de tous les privilèges d'écriture nécessaires pour générer une clé d'API.
- Vous devez disposer d'une clé d'API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir [Générer une clé API](#).)
- Familiarisez-vous avec [Guide de l' API REST ExtraHop](#) pour apprendre à naviguer dans l'explorateur d'API REST d'ExtraHop.

Interrogez les enregistrements via l'explorateur d'API REST

1. Dans un navigateur, accédez à l'explorateur d'API REST.
L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est `seattle-eda`, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Entrez les informations d'identification de votre API REST.
 - Pour les capteurs et les machines virtuelles ECA, cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le **Clé API** champ.
 - Pour RevealX 360, cliquez sur **Entrez les identifiants de l'API** puis collez ou saisissez l'ID et le code secret de vos informations d'identification d'API dans le **IDENTIFIANT** et **Secret** champs.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Journal des enregistrements** puis cliquez sur **POST /enregistrements/recherche**.
5. Cliquez **Essayez-le**.
Le schéma JSON est automatiquement ajouté au corps zone de texte des paramètres.
6. Dans la zone de texte du corps, spécifiez les champs de votre requête d'enregistrement.
Par exemple, les champs suivants récupèrent les enregistrements des 30 dernières minutes qui incluent une adresse IP, un nom de domaine ou un URI qui a été identifié comme suspect selon [renseignement sur les menaces](#):

```
{
  "from": "-30m",
  "filter": {
    "field": "ex.isSuspicious",
    "operator": "=",
    "operand": {
      "type": "boolean",
      "value": "true"
    }
  }
}
```

Pour une liste complète des champs valides, consultez la section Paramètres corporels sous **POST / enregistrements/recherche** dans l'explorateur d'API REST.

Exemples de scripts Python

Les scripts Python suivants recherchent des enregistrements contenant une adresse IP, un nom de domaine ou un URI qui ont été identifiés comme suspects selon les renseignements sur les menaces. Les scripts écrivent ensuite les champs d'enregistrement spécifiés dans un fichier CSV qui peut être consulté dans un tableur.

 **Note:** Pour en savoir plus sur les renseignements sur les menaces avec ExtraHop, voir [Renseignements sur les menaces](#) et [Téléchargez des fichiers STIX via l'API REST](#).

Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements ExtraHop

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait des enregistrements d'un espace de stockage des enregistrements ExtraHop.

Avant de commencer

Cet exemple de script ne prend pas en charge RevealX 360. Pour plus d'informations sur un exemple de script prenant en charge RevealX 360, voir [Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements tiers ou dans le cloud](#).

 **Important:** Si la requête correspond à un nombre supérieur au nombre maximum d'enregistrements pouvant être récupérés simultanément, le script extrait les enregistrements restants en envoyant un curseur à la sonde ou à la console avec l'opération POST / records/cursor. Cette opération n'est valide qu'avec l'espace de stockage des enregistrements ExtraHop. Si vous avez configuré un tiers ou un espace de stockage des enregistrements dans le cloud, consultez [Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements tiers ou dans le cloud](#).

1. Accédez au [Référentiel GitHub d'exemples de code ExtraHop](#) et téléchargez le `query_records_explore/query_records_explore.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `query_records_explore.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
 - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console. Notez que ce nom d'hôte n'est pas le nom d'hôte de l'espace de stockage des enregistrements ExtraHop connecté sur lequel les enregistrements sont stockés.
 - **UN RUCHER:** La clé API.
 - **NOM DE FICHER:** Le fichier dans lequel la sortie est écrite.
 - **LIMITE DE TEMPS:** Si la requête d'enregistrement correspond à plus de 100 enregistrements, durée pendant laquelle les enregistrements restants peuvent être extraits du système après la requête initiale.
 - **REQUÊTE:** Les paramètres de requête d'enregistrement.
 - **COLONNES:** Les champs d'enregistrement qui sont écrits dans le fichier de sortie CSV.
3. Exécutez la commande suivante :

```
python3 query_records_explore.py
```

 **Note:** Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que [un certificat fiable a été ajouté à votre sonde ou à votre console](#). Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```

Récupérez et exécutez l'exemple de script Python pour un espace de stockage des enregistrements tiers ou dans le cloud

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait des enregistrements depuis des magasins d'enregistrements tiers et dans le cloud.



Note: Si la requête correspond à un nombre supérieur au nombre maximum d'enregistrements pouvant être extraits en une seule fois, le script extrait les enregistrements restants en envoyant des requêtes supplémentaires à l'aide du `offset` paramètre. Le paramètre `offset` ignore un nombre spécifié d'enregistrements dans une requête.

1. Accédez au [Référentiel GitHub d'exemples de code ExtraHop](#) et téléchargez le `query_records_third_party/query_records_third_party.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `query_records_third_party.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
 - Pour les capteurs et les machines virtuelles ECA, spécifiez les variables de configuration suivantes :
 - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la machine virtuelle ECA.
 - **CLÉ_API:** La clé API.
 - **NOM DE FICHIER:** Le fichier dans lequel la sortie est écrite.
 - **LIMITE DE TEMPS:** Si la requête d'enregistrement correspond à plus de 100 enregistrements, durée pendant laquelle les enregistrements restants peuvent être extraits du système après la requête initiale.
 - **REQUÊTE:** Les paramètres de requête d'enregistrement.
 - **COLONNES:** Les champs d'enregistrement qui sont écrits dans le fichier de sortie CSV.
 - Pour RevealX 360, spécifiez les variables de configuration suivantes :
 - **HÔTE:** Le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché sur la page d'accès à l'API RevealX 360 sous API Endpoint. Le nom d'hôte n'inclut pas `/oauth2/token`.
 - **IDENTIFIANT:** L'ID des informations d'identification de l'API REST RevealX 360.
 - **SECRET:** Le secret des informations d'identification de l'API REST RevealX 360.
 - **NOM DE FICHIER:** Le fichier dans lequel la sortie est écrite.
 - **LIMITE DE TEMPS:** Si la requête d'enregistrement correspond à plus de 100 enregistrements, durée pendant laquelle les enregistrements restants peuvent être extraits du système après la requête initiale.
 - **REQUÊTE:** Les paramètres de requête d'enregistrement.
 - **COLONNES:** Les champs d'enregistrement qui sont écrits dans le fichier de sortie CSV.
3. Exécutez la commande suivante :

```
python3 query_records_third_party.py
```



Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que **un certificat fiable a été ajouté à votre sonde ou à votre console**. Vous pouvez également ajouter `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

```
requests.get(url, headers=headers, verify=False)
```