

Configurer AlienVault comme source de menaces externes pour ESA

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Qu'est-ce que STIX/TAXII ?](#)

[STIX \(Structured Threat Information Expression\)](#)

[TAXII \(Trusted Automated Exchange of Intelligence Information\)](#)

[Sources d'alimentation](#)

[Bibliothèque Cabby](#)

[Installation de Cabby Library](#)

[AlienVault - Impulsions et flux](#)

[Impulsions](#)

[Flux](#)

[Commencer à interroger les collections](#)

[Interrogation depuis son propre profil](#)

[Interrogation à partir des profils AlienVault](#)

[Abonnements à AlienVault Profile Collection](#)

[Ajout de sources à ESA](#)

[Ajout de source sans flux](#)

[Source d'interrogation sans flux](#)

[Vérifier](#)

[Ajout d'une source avec des flux](#)

[Source d'interrogation avec flux](#)

[Vérifier](#)

Introduction

Ce document décrit les étapes à suivre pour configurer des flux de menaces externes à partir d'une source AlienVault et l'utiliser dans ESA.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Cisco Secure Email Gateway (SEG / ESA) AsyncOS 16.0.2
- CLI Linux
- Python3 pip
- Compte AlienVault

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Dispositif de sécurité de la messagerie
- Python3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le cadre ETF (External Threat Feeds) permet à la passerelle de messagerie d'acquérir des informations sur les menaces externes partagées au format STIX via le protocole TAXII. En tirant parti de cette fonctionnalité, les entreprises peuvent :

- Adoptez une position proactive contre les cybermenaces telles que les programmes malveillants, les ransomwares, le phishing et les attaques ciblées.
- Abonnez-vous à des sources de renseignements sur les menaces locales et tierces.
- Améliorez l'efficacité globale de la passerelle de messagerie.

Qu'est-ce que STIXX/TAXII ?

STIX (Structured Threat Information Expression)

STIX est un format normalisé utilisé pour décrire les informations sur les cybermenaces (CTI), notamment les indicateurs, les tactiques, les techniques, les programmes malveillants et les acteurs de la menace, de manière structurée et lisible par machine. Un flux STIX inclut généralement des indicateurs, des modèles qui aident à détecter les activités cybernétiques suspects ou malveillantes.

TAXII (Trusted Automated Exchange of Intelligence Information)

TAXII est un protocole utilisé pour échanger des données STIX entre des systèmes de manière sécurisée et automatique. Définit la manière dont les informations sur les cybermenaces sont échangées entre les systèmes, les produits ou les organisations via des services dédiés (serveurs TAXII).



Remarque : la version 16.0 d'AsyncOS prend en charge les versions STIX/TAXII : STIX 1.1.1 et 1.2, avec TAXII 1.1.

Sources d'alimentation

Les appliances de sécurité de la messagerie électronique peuvent utiliser des flux de renseignements sur les menaces provenant de diverses sources, notamment des référentiels publics, des fournisseurs commerciaux et leurs propres serveurs privés au sein de votre entreprise.

Pour garantir la compatibilité, toutes les sources doivent utiliser les normes STIX/TAXII, qui permettent un partage structuré et automatisé des données sur les menaces.

Bibliothèque Cabby

La bibliothèque Cabby Python est un outil utile pour se connecter aux serveurs TAXII, découvrir les collections STIX et interroger les données sur les menaces. Il s'agit d'un excellent moyen de tester et de valider le bon fonctionnement d'une source de flux et de renvoyer les données comme prévu avant de les intégrer à votre appliance de sécurité de la messagerie.

Installation de Cabby Library

Pour installer la bibliothèque Cabby, vous devez vous assurer que votre machine locale a Python pip installé.

Une fois que python pip est installé, il vous suffit d'exécuter cette commande pour installer la bibliothèque cabby.

```
python3 -m pip install cabby
```

Une fois l'installation de la bibliothèque cabby terminée, vous pouvez vérifier que les commandes taxi-collections et taxi-poll sont maintenant disponibles.

```
(cabby) bash-3.2$ taxii-collections -h
usage: taxii-collections [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https]
                        [--cert CERT] [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME]
                        [--proxy-url PROXY_URL] [--proxy-type {http,https}] [--header HEADERS] [-v] [-]
```

```
(cabby) bash-3.2$ taxii-poll -h
usage: taxii-poll [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https] [--verbose]
                 [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME] [--password PASSWORD]
                 [--proxy-type {http,https}] [--header HEADERS] [-v] [-x] [-t {1.0,1.1}] [-c COLLECTION]
                 [-b BINDINGS] [-s SUBSCRIPTION_ID] [--count-only]
```

AlienVault - Impulsions et flux

Pour commencer à découvrir les informations AlienVault, créez d'abord un compte sur le site AlienVault, puis commencez à rechercher les informations souhaitées.

Dans AlienVault, les flux et les impulsions sont liés, mais pas les mêmes :

Impulsions

Les impulsions sont organisées par des informations sur les menaces avec des indicateurs groupés + contexte (lisible par l'homme).

- Une impulsion est un ensemble d'indicateurs de menace (IOC) regroupés autour d'une menace ou d'une campagne spécifique.
- Créé par la communauté ou les fournisseurs pour décrire des éléments tels que les programmes malveillants, le phishing et les ransomwares.
- Chaque impulsion inclut une description contextuelle des menaces, des indicateurs associés (IP, domaine, hachage de fichier, etc.), des balises et des références.
- Les impulsions sont lisibles par l'homme et structurées de manière à pouvoir être facilement comprises et partagées.

Imaginez une impulsion comme un rapport de menace avec des indicateurs de compromission et des métadonnées groupés.

Flux

Les flux sont des flux automatisés d'indicateurs à partir de plusieurs impulsions (lisibles par machine).

- Les flux sont un flux d'indicateurs bruts (IOC) extraits d'une ou de plusieurs impulsions, généralement de manière automatisée.
- Ils sont généralement utilisés par les outils de sécurité pour ingérer des indicateurs en masse, via des formats tels que STIX/TAXII, CSV ou JSON.
- Les flux sont axés sur les machines et utilisés pour l'automatisation et l'intégration avec les SIEM, les pare-feu et les passerelles de messagerie.

Un flux concerne davantage le mécanisme de distribution, tandis qu'une impulsion est le contenu et le contexte de la menace.

Vous interrogez généralement des flux, et ces flux sont composés d'indicateurs extraits d'impulsions.

Commencer à interroger les collections

Interrogation depuis son propre profil

Une fois que vous avez votre compte AlienVault, vous pouvez commencer à utiliser les commandes taxi-collections et taxi-poll.

Voici comment utiliser ces commandes pour cet exemple d'utilisation :

Dans ce cas, dans le profil AlienVault, il n'y a pas d'impulsions disponibles, mais comme un test, vous pouvez interroger une collection de votre profil en utilisant la commande taxi-poll :



PROFILE

Personal profile

 0 pulses

 0 contributions

profil personnel alienvault

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_
```

```
--username abcdefg --password ****
```

```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\  
> --username [REDACTED] --password [REDACTED]  
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL  
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll  
2025-05-27 12:13:41,51; INFO: 0 blocks polled
```

profil personnel d'enquête

Comme vous pouvez le voir, aucun bloc n'est interrogé car aucune information n'est disponible dans le profil AlienVault.

Interrogation à partir des profils AlienVault

Une fois que les profils à l'intérieur d'AlienVault sont découverts, certains d'entre eux ont des impulsions. Dans cet exemple, le profil AlienVault est utilisé.



PROFILE

ALIENVAULT

Follow

Unsubscribe



7176 pulses



326 contributions

profil alienvault

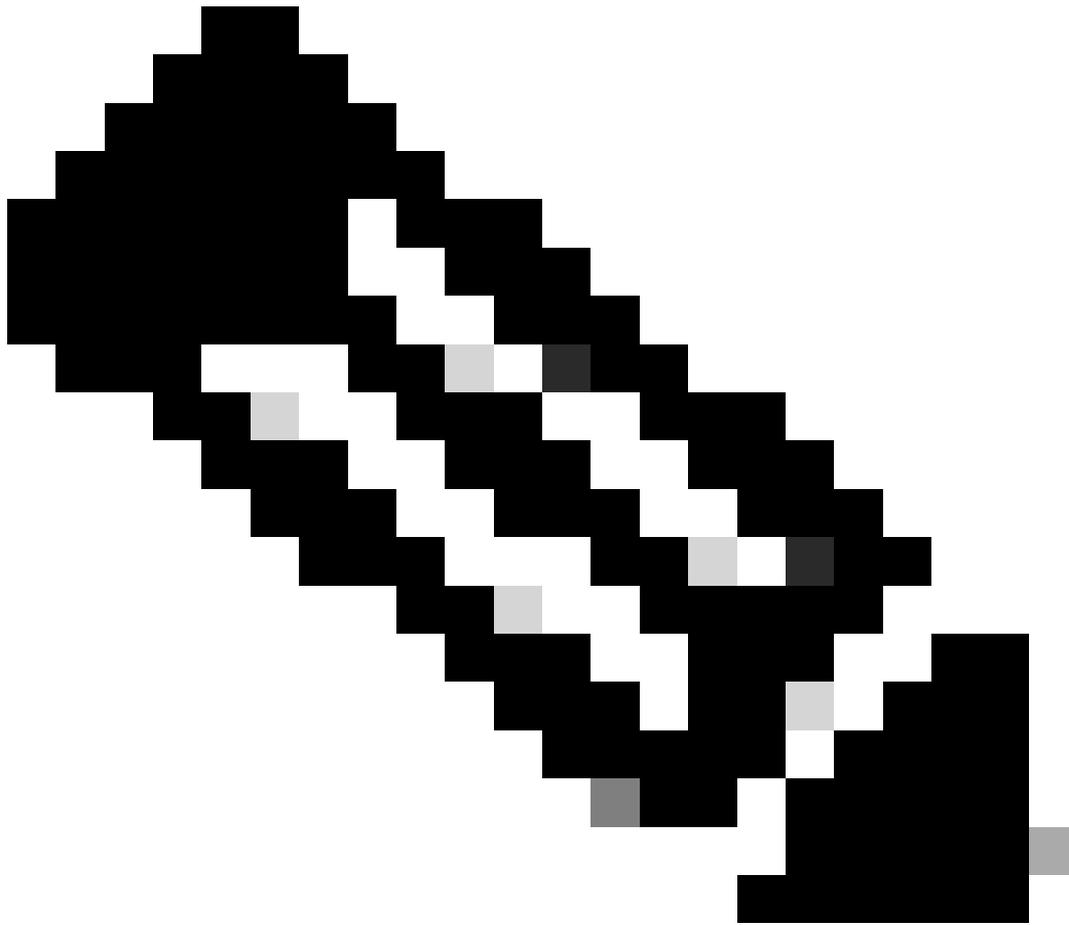
Lors de l'exécution de l'interrogation avec la commande taxi-poll, il commence immédiatement à lire toutes les informations du profil.

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_AlienVault --username abcdefg
```

```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_AlienVault  
> --username [REDACTED] --password anything  
2025-05-27 12:14:04,048 INFO: Polling using data binding: ALL  
2025-05-27 12:14:04,048 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll  
<stix:STIX_Package xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:DomainNameObj="http://
```

sondage alienvault

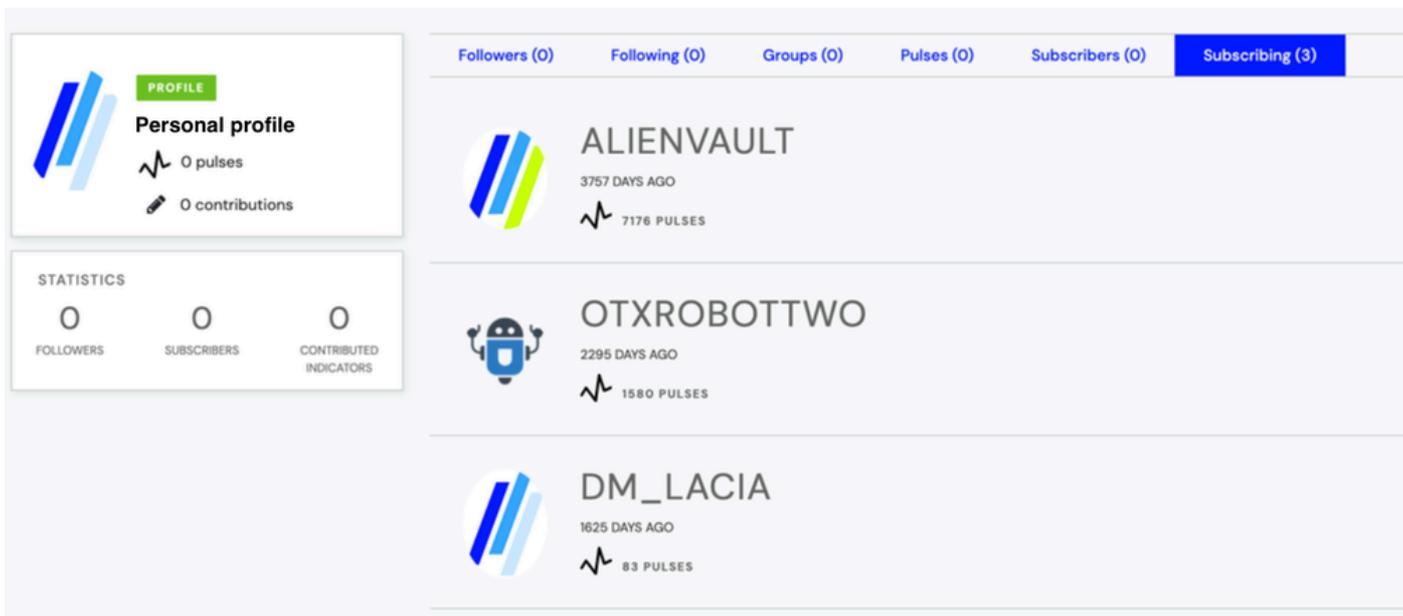
Comme indiqué, le processus commence à extraire les informations.



Remarque : Pour connaître votre nom d'utilisateur et votre mot de passe, cliquez sur le lien <https://otx.alienvault.com/api>

Abonnements à AlienVault Profile Collection

À titre de test, cet utilisateur s'est abonné à 3 profils.



abonnements aux profils personnels

Vous pouvez utiliser la commande taxi-collections pour récupérer ces abonnements.

taxii-collections --path https://otx.alienvault.com/taxii/collections --username abcdefg --password ***

```
(cabby) bash-3.2$ taxii-collections --path https://otx.alienvault.com/taxii/collections --username [redacted] --password [redacted]
ord anything
2025-05-28 09:57:45.751 INFO: Sending Collection_Information_Request to https://otx.alienvault.com/taxii/collections
=== Data Collection Information ===
Collection Name: user_AlienVault
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: AlienVault
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_diegoher
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: diegoher
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_dm_lacia
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: dm_lacia
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_otxrobottwo
Collection Type: DATA_FEED
Available: True
```

collections de profils personnels

Vous pouvez confirmer que la commande taxi-collections fonctionne si le nom de la collection est

identique à celui auquel vous êtes abonné.

Ajout de sources à ESA

Ajout de source sans flux

1. Accédez à Politiques de messagerie > Gestionnaire des sources de menaces externes.
2. Passez en mode cluster.
3. Cliquez sur Ajouter une source.
4. Nom de l'hôte: otx.alienvault.com
5. Chemin d'interrogation : /taxi/poll
6. Nom de la collection : user_<nom_utilisateur_AlienVault>
7. Port : 443
8. Configurer les identifiants utilisateur : Celui qu'AlienVault vous a fourni.
9. Cliquez sur Submit > Commit Changes.

Edit Source

Mode —Cluster: Hosted_Cluster Change Mode...

▸ Centralized Management Options

The settings below are for the configuration of STIX over TAXII sources only.

Source Details	
Source Name:	<input type="text" value="alienvault_diegoher"/>
Description (Optional):	<input type="text"/>
TAXII Details	
Hostname: ?	<input type="text" value="otx.alienvault.com"/>
Polling Path: ?	<input type="text" value="/taxii/poll"/>
Collection Name: ?	<input type="text" value="user_diegoher"/>
Polling interval:	<input type="text" value="1"/> Hours <input type="text" value="0"/> mins <i>(Maximum 24 Hours.)</i>
Age of Threat Feeds: ?	<input type="text" value="30"/> Days <i>(Maximum 365 Days.)</i>
Time Span of Poll Segment ?	<input type="text" value="30"/> Days <i>The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.</i>
Use HTTPS:	<input checked="" type="radio"/> Yes <input type="radio"/> No Polling Port: ? <input type="text" value="443"/>
Configure User Credentials:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Basic Authentication Username: <input type="text" value="xyz"/> Password: <input type="password" value="....."/>
Proxy Details	
Use Global Proxy:	<input type="radio"/> Yes <input checked="" type="radio"/> No <i>To configure Proxy Server, go to: Security Services > Security Updates</i>

source personnelle

Source d'interrogation sans flux

Dans le Gestionnaire des sources de menaces externes, une fois la source ajoutée, la nouvelle source devient visible.

External Threat Feeds Manager

Mode — **Cluster: Hosted_Cluster** Change Mode...

▸ Centralized Management Options

External Threat Feed Sources

[Add Source](#)

alienvault_diegoher	Hostname otx.alienvault.com	1h	10 Jun 2025 12:43:56	Idle			Poll Now
	Collection Name user_diegoher						

* You can configure up to 8 external threat feed sources only.

Key: Polling Suspended

aliment personnel

Une fois ajouté, cliquez sur Sondage maintenant.

Vérifier

Connectez-vous à l'ESA via l'interface de ligne de commande et consultez les journaux des menaces pour vérifier les informations.

```
THREAT_FEEDS: A delta poll is scheduled for the source: alienvault_diegoher
THREAT_FEEDS: A delta poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_diegoher
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-06-10 10:22:33.058477 and 2025-06-10
THREAT_FEEDS: No new observables were fetched from the source: alienvault_diegoher
THREAT_FEEDS: 0 observables were fetched from the source: alienvault_diegoher
```

sondage individuel ETF

Comme le montre l'image, vous pouvez voir que 0 observable a été récupéré et c'est attendu parce qu'il n'y a pas de flux dans le profil montré.

Ajout d'une source avec des flux

1. Accédez à Politiques de messagerie > Gestionnaire des sources de menaces externes.
2. Passez en mode cluster.
3. Cliquez sur Ajouter une source.
4. Nom de l'hôte: otx.alienvault.com
5. Chemin d'interrogation : /taxi/poll
6. Nom de la collection : utilisateur_AlienVault
7. Port : 443
8. Configurer les identifiants utilisateur : Celui qu'AlienVault vous a fourni.
9. Cliquez sur Submit > Commit Changes.

Edit Source

Mode —Cluster: Hosted_Cluster Change Mode...

▸ Centralized Management Options

The settings below are for the configuration of STIX over TAXII sources only.

Source Details	
Source Name:	<input type="text" value="alienvault_diegoher"/>
Description (Optional):	<input type="text"/>
TAXII Details	
Hostname: ?	<input type="text" value="otx.alienvault.com"/>
Polling Path: ?	<input type="text" value="/taxii/poll"/>
Collection Name: ?	<input type="text" value="user_AlienVault"/>
Polling interval:	<input type="text" value="1"/> Hours <input type="text" value="0"/> mins <i>(Maximum 24 Hours.)</i>
Age of Threat Feeds: ?	<input type="text" value="30"/> Days <i>(Maximum 365 Days.)</i>
Time Span of Poll Segment ?	<input type="text" value="30"/> Days <i>The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.</i>
Use HTTPS:	<input checked="" type="radio"/> Yes <input type="radio"/> No Polling Port: ? <input type="text" value="443"/>
Configure User Credentials:	<input checked="" type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Basic Authentication Username: <input type="text" value="xyz"/> Password: <input type="password" value="....."/>
Proxy Details	
Use Global Proxy:	<input type="radio"/> Yes <input checked="" type="radio"/> No <i>To configure Proxy Server, go to: Security Services > Security Updates</i>

source alienvault

Source d'interrogation avec flux

Dans le Gestionnaire des sources de menaces externes, une fois la source ajoutée, la nouvelle source devient visible.

External Threat Feeds Manager

Mode — Cluster: Hosted_Cluster Change Mode...

▸ Centralized Management Options

External Threat Feed Sources

[Add Source](#)

alienvault_diegoher	Hostname otx.alienvault.com	1h	10 Jun 2025 12:43:56	Idle	⏸	🗑	Poll Now
	Collection Name user_AlienVault						

* You can configure up to 8 external threat feed sources only.

Key: Polling Suspended

alimentation alienvault

Une fois ajouté, cliquez sur Sondage maintenant.

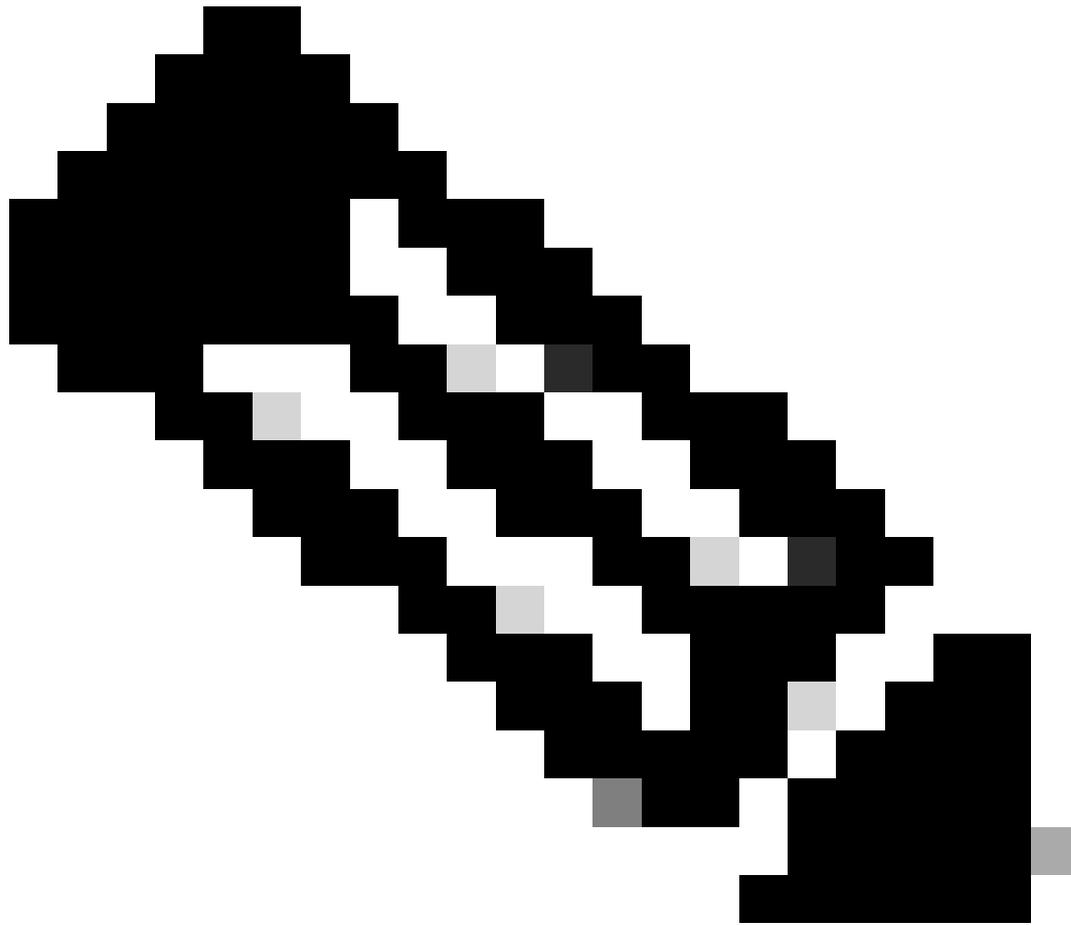
Vérifier

Connectez-vous à l'ESA via l'interface de ligne de commande et consultez les journaux des menaces pour vérifier les informations.

```
THREAT_FEEDS: A full poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_AlienVault
THREAT_FEEDS: All feeds from the source: alienvault_diegoher has been purged successfully.
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-05-11 12:43:56.235896 and 2025-06-10
THREAT_FEEDS: The external threat feeds engine has started
THREAT_FEEDS: 6757 observables were fetched from the source: alienvault_diegoher
```

interrogation du flux alienvault

Comme le montre l'image, vous pouvez voir que plusieurs observables ont été récupérés.



Remarque : Si de nouveaux flux sont ajoutés à la collection configurée, l'ESA interroge automatiquement la source et les nouveaux observables sont récupérés.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.