AlienVault configureren als externe bedreigingsfeed voor ESA

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het configureren van externe bedreigingsfeeds vanuit een AlienVault-bron en het gebruik ervan binnen het ESA.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- e-mailbeveiligingstoestel
- Python3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het External Threat Feeds (ETF) framework maakt het mogelijk dat de e-mailgateway externe dreigingsinformatie kan opnemen die via het TAXII-protocol in STIX-formaat wordt gedeeld. Door gebruik te maken van deze mogelijkheden kunnen organisaties:

- Neem een proactieve houding aan tegen cyberdreigingen zoals malware, ransomware, phishing en gerichte aanvallen.
- Abonneer u op zowel lokale als externe bronnen van bedreigingsinformatie.
- Verbeter de algehele effectiviteit van de e-mailgateway.

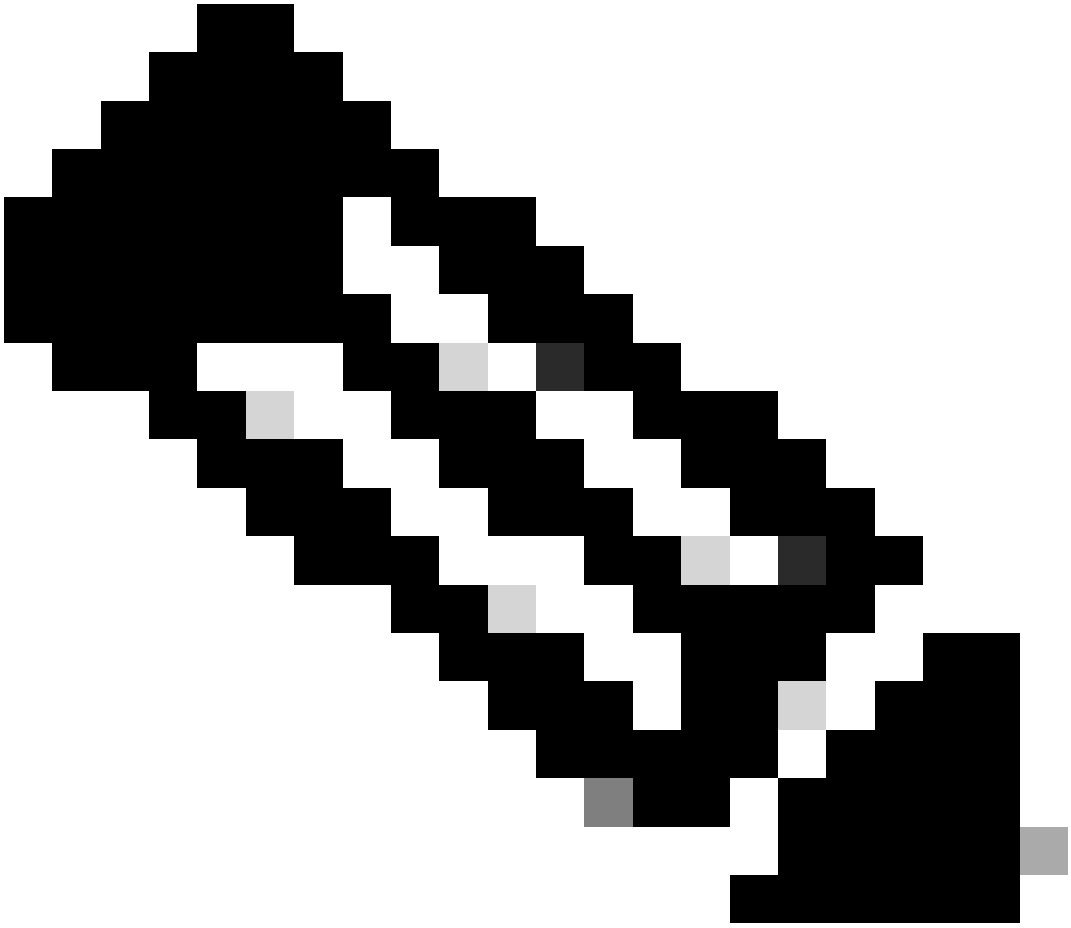
Wat is STIXX/TAXII?

STIX (Structured Threat Information Expression)

STIX is een gestandaardiseerd formaat dat wordt gebruikt om cyberdreigingsinformatie (CTI) - inclusief indicatoren, tactieken, technieken, malware en bedreigingsactoren - op een gestructureerde en machineleesbare manier te beschrijven. Een STIX-feed bevat meestal indicatoren - patronen die helpen verdachte of schadelijke cyberactiviteiten te detecteren.

TAXII (Trusted Automated Exchange of Intelligence Information)

TAXII is een protocol dat wordt gebruikt om STIX-gegevens veilig en automatisch tussen systemen uit te wisselen. Bepaalt hoe informatie over cyberdreigingen wordt uitgewisseld tussen systemen, producten of organisaties via speciale services (TAXII-servers).



Opmerking: AsyncOS 16.0 release ondersteunt STIX / TAXII versies: STIX 1.1.1 en 1.2, met TAXII 1.1.

Voederbronnen

E-mailbeveiligingstoestellen kunnen feeds van bedreigingsinformatie uit verschillende bronnen gebruiken, waaronder openbare opslagplaatsen, commerciële providers en hun eigen privéservers binnen uw organisatie.

Om de compatibiliteit te waarborgen, moeten alle bronnen de STIX/TAXII-normen gebruiken, die een gestructureerde, geautomatiseerde uitwisseling van bedreigingsgegevens mogelijk maken.

Cabby-bibliotheek

De Cabby Python-bibliotheek is een handig hulpmiddel voor het verbinden met TAXII-servers, het ontdekken van STIX-verzamelingen en het peilen van bedreigingsgegevens. Het is een geweldige manier om te testen en te valideren dat een feedbron correct werkt en gegevens retourneert zoals verwacht voordat u deze in uw e-mailbeveiligingsapparaat integreert.

Cabby Library installeren

Om de Cabby-bibliotheek te installeren, moet u ervoor zorgen dat uw lokale machine Python-pip heeft geïnstalleerd.

Zodra python pip is geïnstalleerd, hoeft u alleen maar deze opdracht uit te voeren om de kabelbibliotheek te installeren.

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

Zodra de installatie van de kabelbibliotheek is voltooid, kunt u controleren of de opdrachten taxii-collecties en taxii-poll nu beschikbaar zijn.

```
(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] [--ve
                  [--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 - pulsen en feeds

Als u wilt beginnen met het ontdekken van AlienVault-informatie, maakt u eerst een account op de AlienVault-site en begint u vervolgens te zoeken naar de informatie die u wilt.

In AlienVault zijn feeds en pulsen gerelateerd, maar niet hetzelfde:

Pulsen

Pulsen zijn samengestelde bedreigingsinformatie met gegroepeerde indicatoren + context (leesbaar voor de mens).

- Een Pulse is een verzameling van dreigingsindicatoren (IOC's) gegroepeerd rond een specifieke dreiging of campagne.
- Gemaakt door de gemeenschap of providers om dingen zoals malware, phishing, ransomware te beschrijven.
- Elke puls bevat context zoals bedreigingsbeschrijving, bijbehorende indicatoren (IP, domein, bestandshash enzovoort), tags en verwijzingen.
- Pulsen zijn menselijk leesbaar en gestructureerd op een manier die gemakkelijk kan worden begrepen en gedeeld.

Zie een puls als een dreigingsrapport met gegroepeerde IOC's en metagegevens.

Feeds

Feeds zijn geautomatiseerde stroom van indicatoren van meerdere pulsen (machineleesbaar).

- Feeds zijn een stroom van ruwe indicatoren (IOC's) getrokken uit een of meer pulsen, meestal op een geautomatiseerde manier.
- Ze worden meestal gebruikt door beveiligingshulpmiddelen om indicatoren in bulk in te nemen, via formaten zoals STIX / TAXII, CSV of JSON.
- Feeds zijn machine-gericht en worden gebruikt voor automatisering en integratie met SIEM's, firewalls en e-mailgateways.

Een feed gaat meer over het afgiftemechanisme, terwijl een puls de inhoud en context van de dreiging is.

Je peilt meestal feeds en die feeds bestaan uit indicatoren die uit pulsen worden geëxtraheerd.

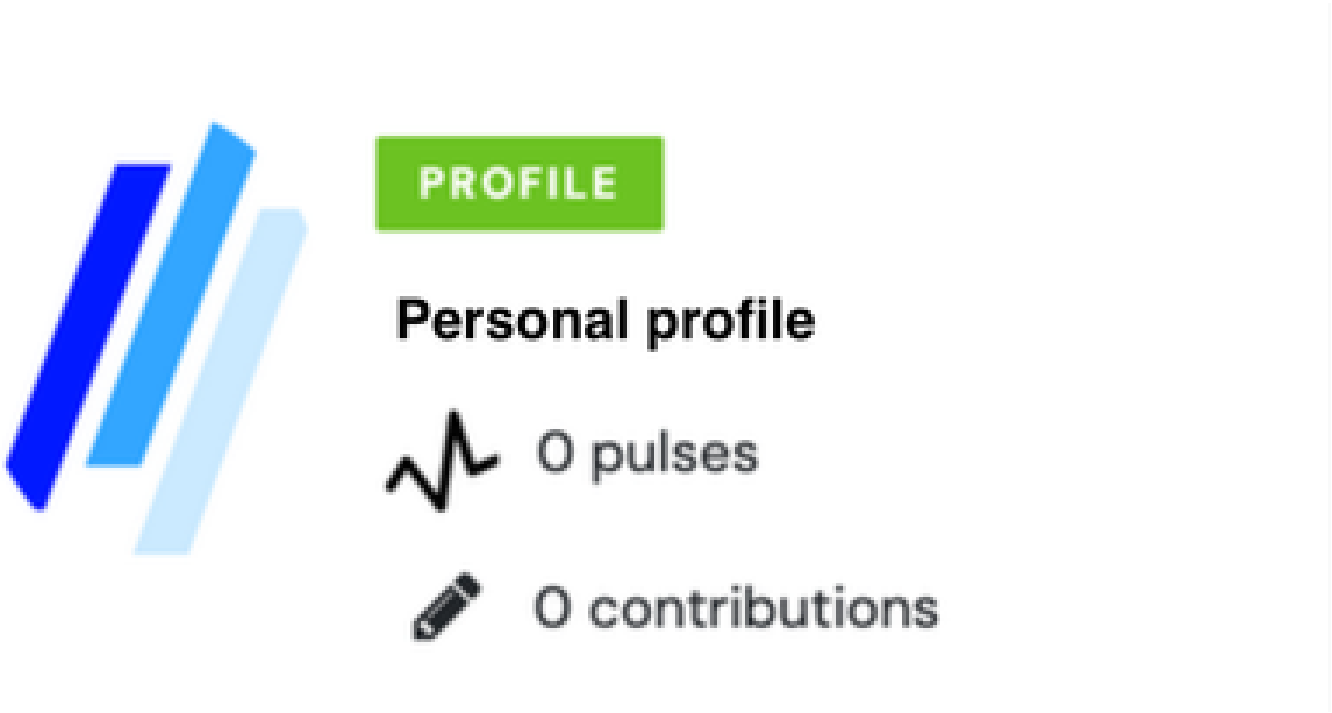
Begin met polling collecties

Polling uit eigen profiel

Zodra u uw AlienVault-account hebt, kunt u beginnen met het gebruik van de taxiverzamelingen en taxipoll-opdrachten.

Zo gebruikt u deze opdrachten voor deze use case:

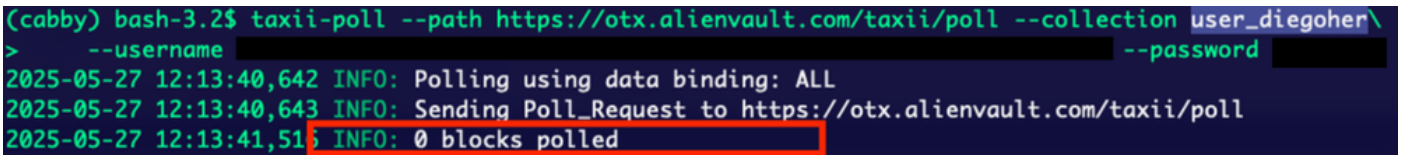
In dit geval zijn er binnen het AlienVault-profiel geen pulsen beschikbaar, maar als test kunt u een verzameling uit uw profiel pollen met de opdracht taxipoll:



Persoonlijk profiel van Alienvault

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

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

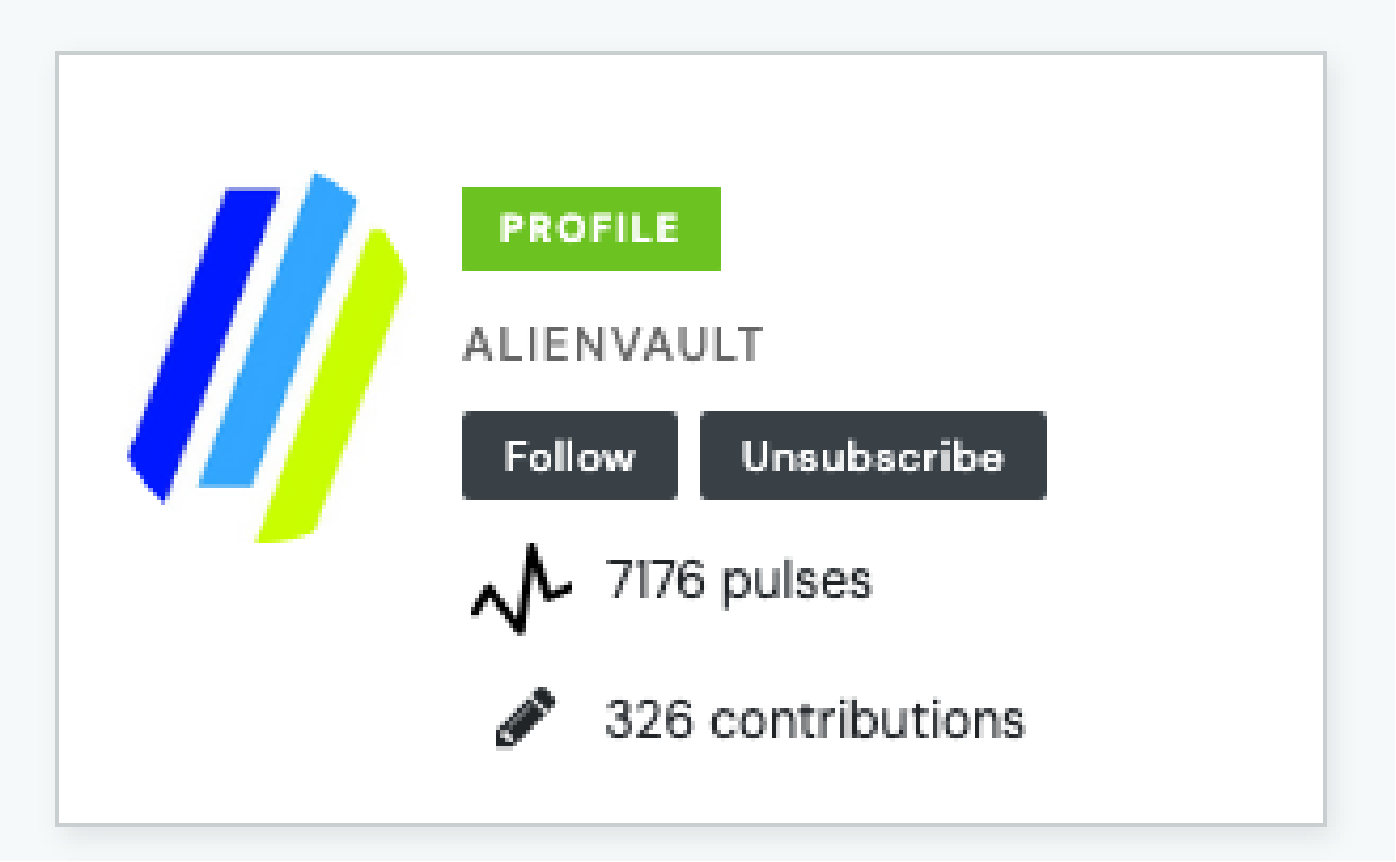


Persoonlijk profiel poll

Zoals u kunt zien, zijn er geen gepolste blokken omdat er geen informatie beschikbaar is in het AlienVault-profiel.

Polling van AlienVault-profielen

Zodra profielen in AlienVault zijn ontdekt, hebben sommige van hen pulsen. In dit voorbeeld wordt het AlienVault-profiel gebruikt.



Alienvault-profiel

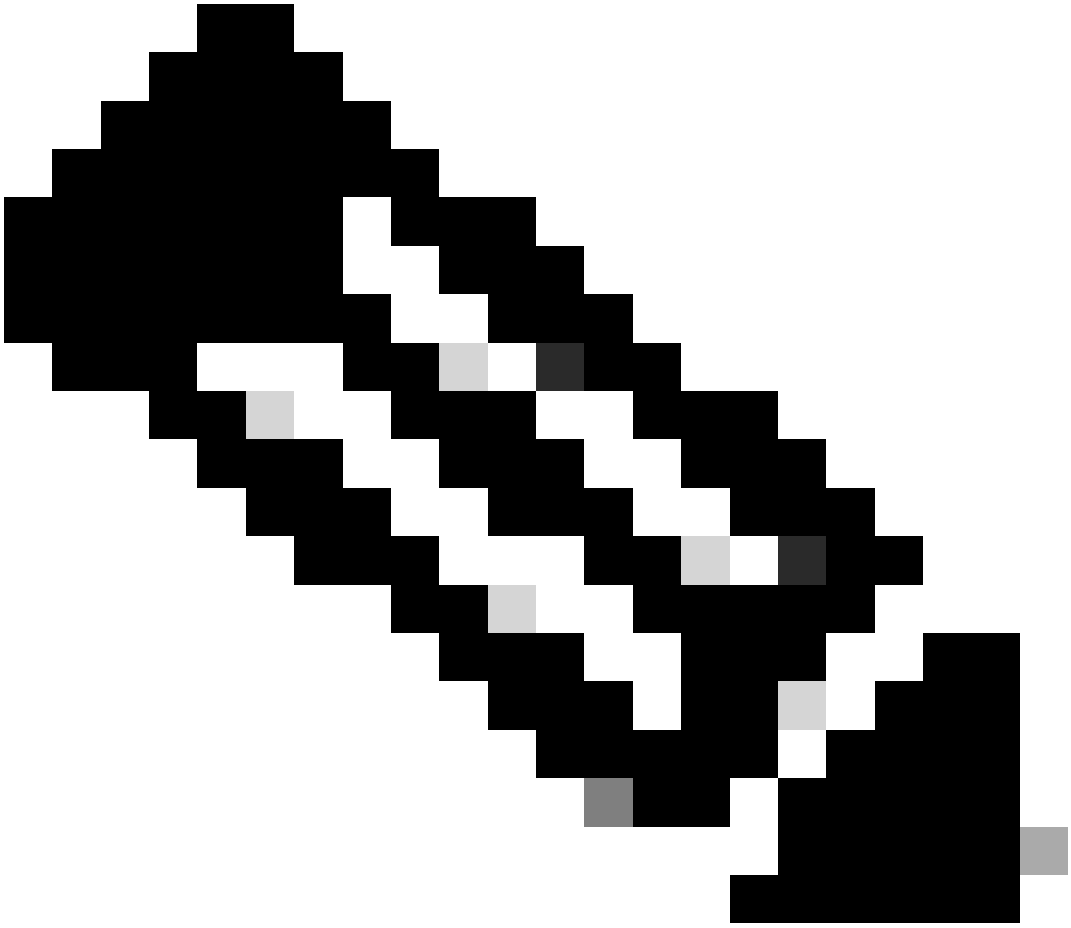
Wanneer de poll wordt uitgevoerd met de opdracht taxipoll, begint deze onmiddellijk alle informatie uit het profiel op te halen.

```
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:/
```

Alienvault-poll

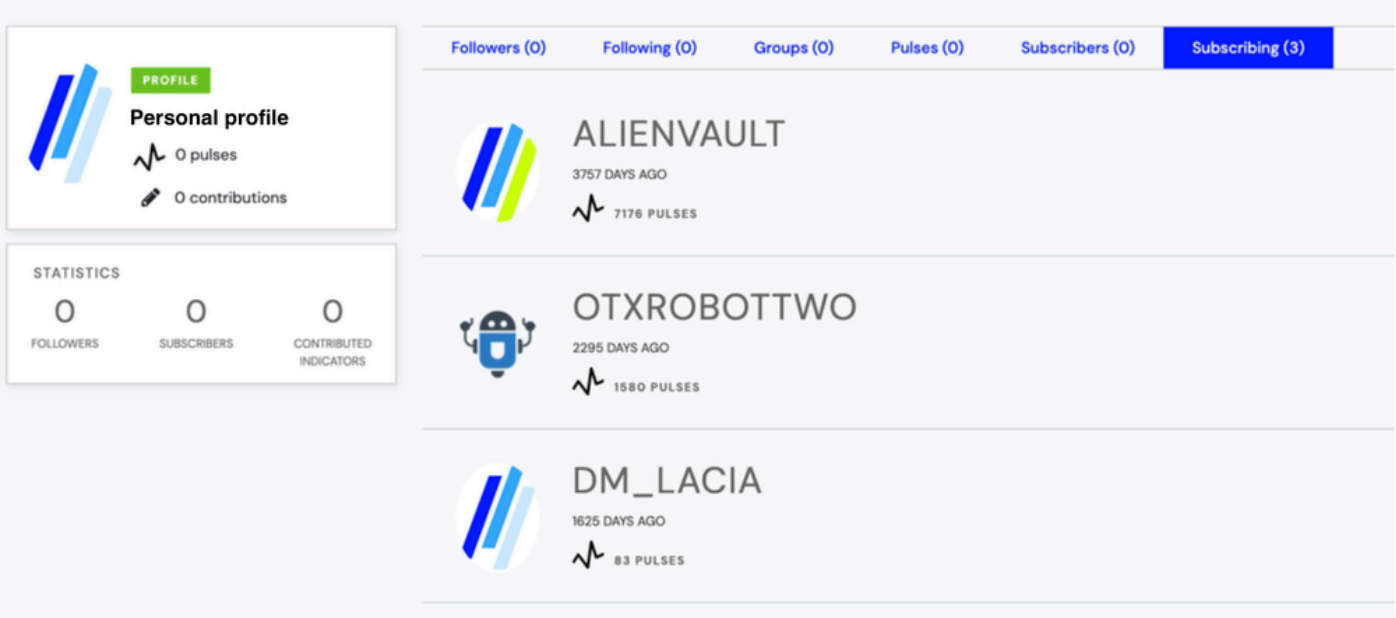
Zoals getoond begint het proces met het ophalen van de informatie.



Opmerking: Om te weten wat uw gebruikersnaam en wachtwoord is, vinkt u deze link aan https://otx.alienvault.com/api

AlienVault Profile Collection-abonnementen

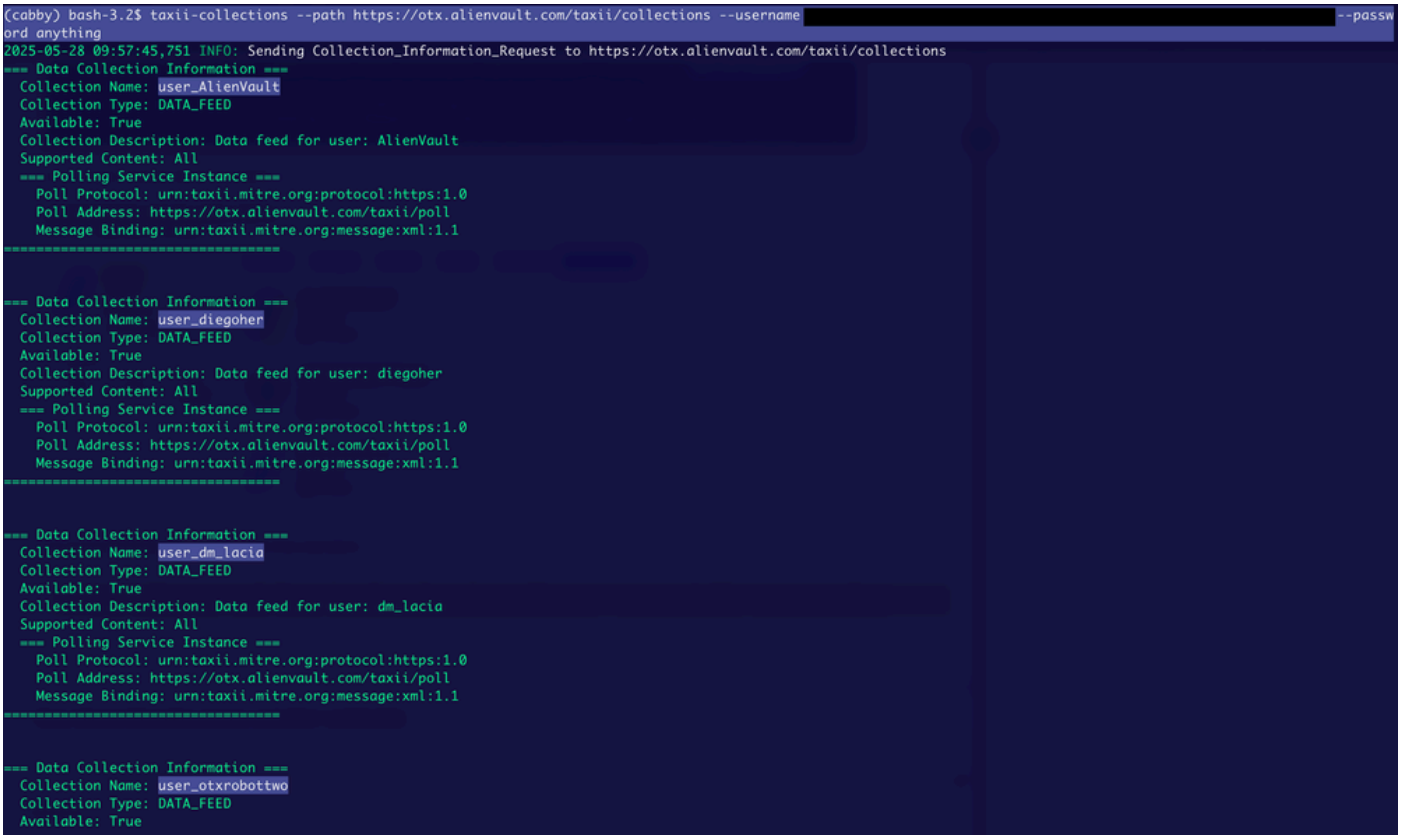
Als test heeft deze gebruiker zich geabonneerd op 3 profielen.



Abonnementen op persoonlijke profielen

U kunt de opdracht taxiverzamelingen gebruiken om die abonnementen op te halen.

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



Persoonlijke profielcollecties

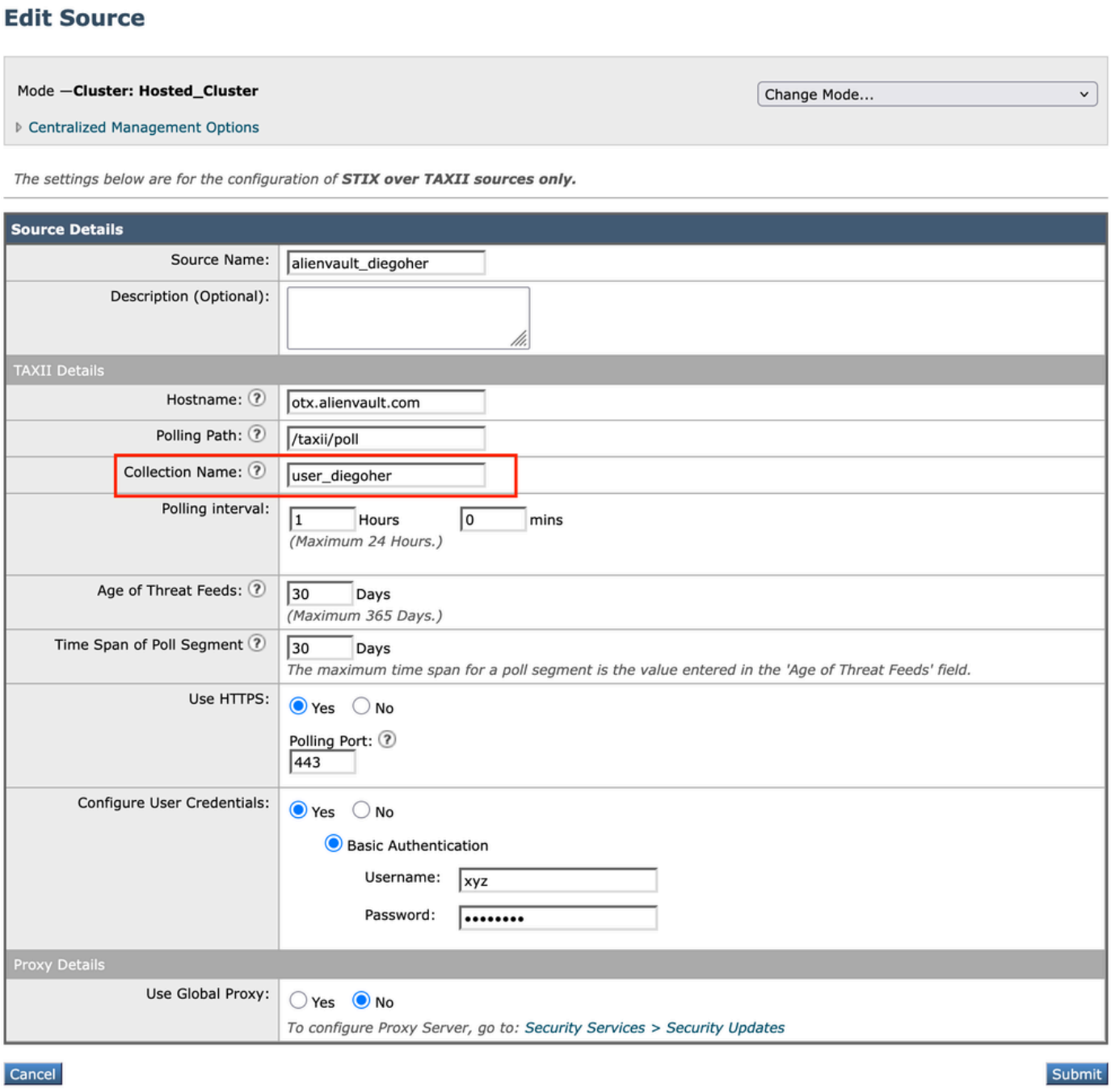
U kunt bevestigen dat de opdracht taxii-collections werkt als de verzamelnaam dezelfde is als de

naam waarop u bent geabonneerd.

Bronnen toevoegen aan ESA

Bron toevoegen zonder feeds

1. Navigeer naar E-mailbeleid > Externe Threat Feeds Manager.
2. Wijzigen in clustermodus.
3. Klik op Bron toevoegen.
4. Hostnaam: otx.alienvault.com
5. Polling Path: /taxi/poll
6. Verzamelnaam: gebruiker_<your_AlienVault_username>
7. Poort: 443
8. Gebruikersreferenties configureren: degene die AlienVault aan u heeft geleverd.
9. Klik op Indienen > Wijzigingen vastleggen.



persoonlijke bron

Peilingbron zonder feeds

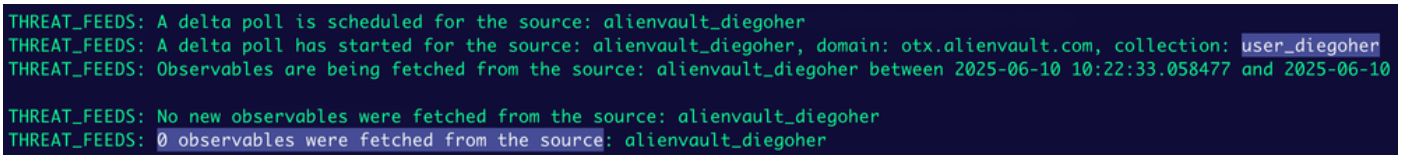
In de External Threat Feeds Manager wordt, nadat de bron is toegevoegd, de nieuw toegevoegde bron zichtbaar.

persoonlijke voeding

Eenmaal toegevoegd, klik je op Poll Now.

Verifiëren

Meld u aan bij de ESA via CLI en bekijk de logboeken van bedreigde feeds om de informatie te verifiëren.

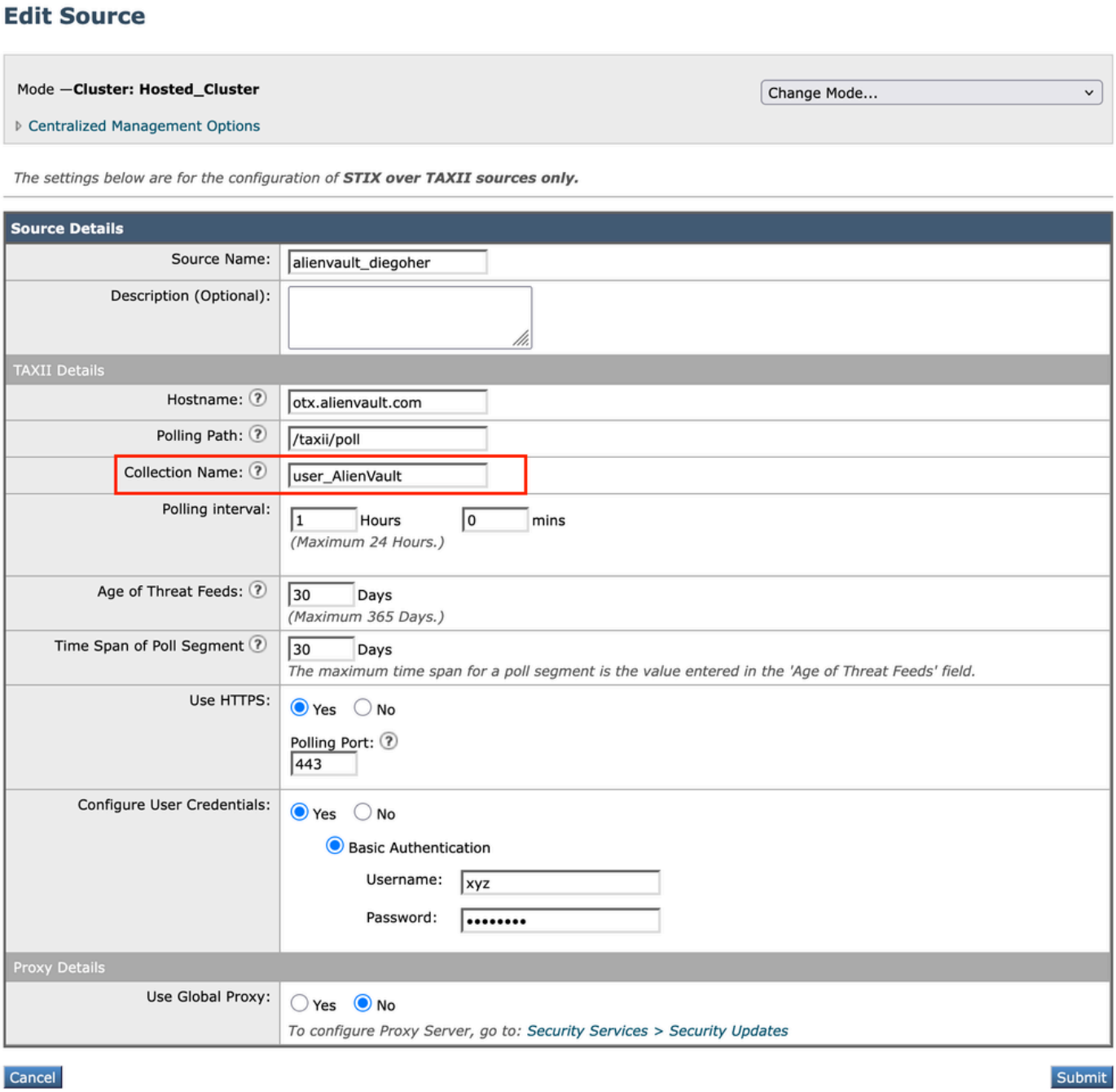


ETF persoonlijke poll

Zoals in de afbeelding te zien is kun je zien dat er 0 observables zijn opgehaald en dit is te verwachten omdat er geen feeds in het getoonde profiel staan.

Bron toevoegen met feeds

1. Navigeer naar E-mailbeleid > Externe Threat Feeds Manager.
2. Wijzigen in clustermodus.
3. Klik op Bron toevoegen.
4. Hostnaam: otx.alienvault.com
5. Polling Path: /taxi/poll
6. Collectienaam: user_AlienVault
7. Poort: 443
8. Gebruikersreferenties configureren: degene die AlienVault aan u heeft geleverd.
9. Klik op Indienen > Wijzigingen vastleggen.



Alienvault-bron

Polling-bron met feeds

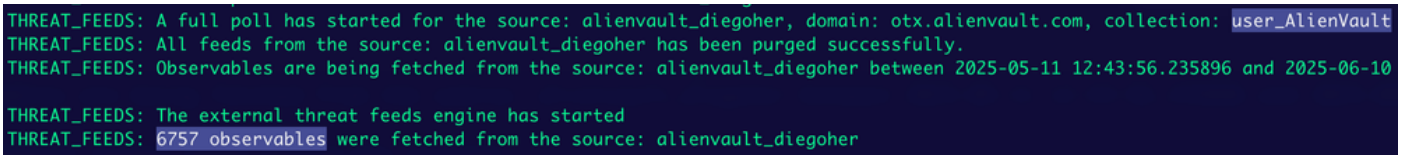
In de External Threat Feeds Manager wordt, nadat de bron is toegevoegd, de nieuw toegevoegde bron zichtbaar.

Alienvault-toevoer

Eenmaal toegevoegd, klik op Poll Now.

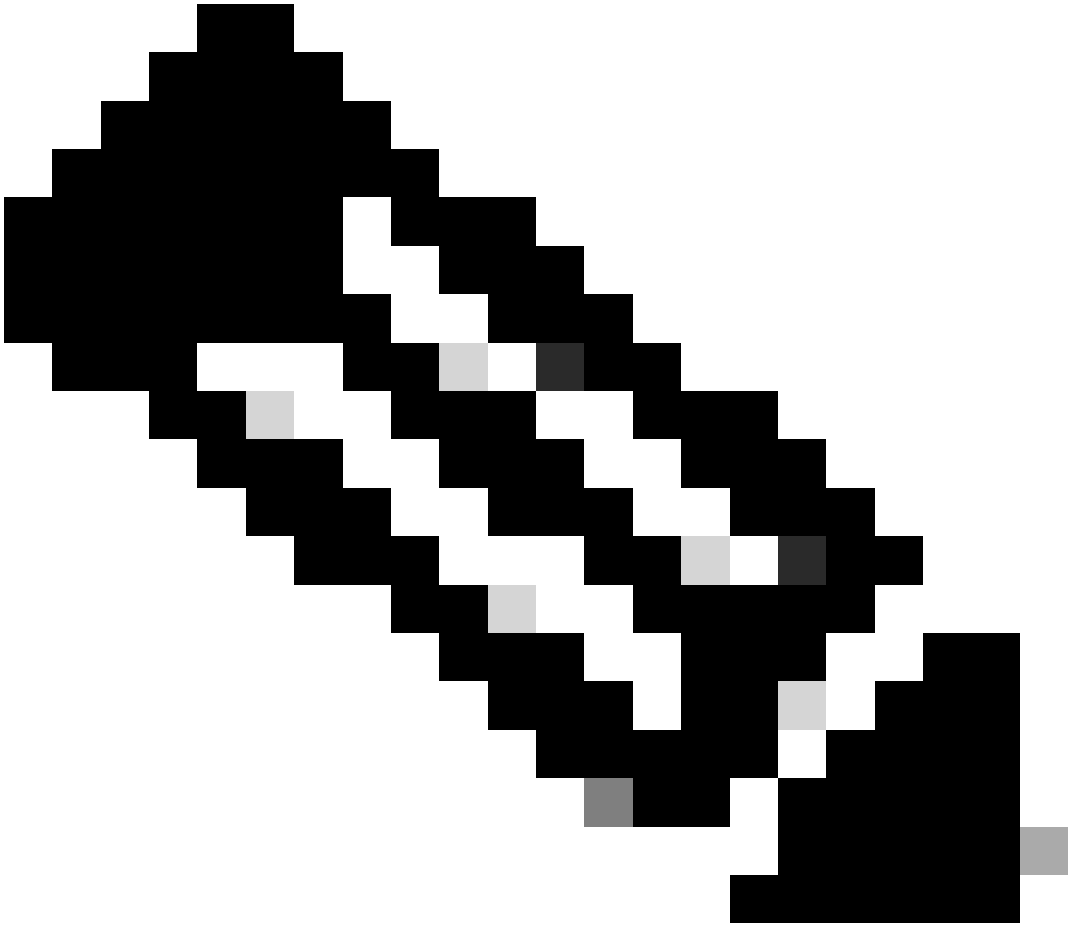
Verifiëren

Meld u aan bij de ESA via CLI en bekijk de logboeken van bedreigde feeds om de informatie te verifiëren.



Alienvault-voeding voor polling

Zoals in de afbeelding te zien is, zijn er meerdere observables opgehaald.



Opmerking: Als nieuwe feeds worden toegevoegd aan de geconfigureerde collectie, peilt de ESA automatisch de bron en worden de nieuwe observables opgehaald.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.