Configurazione di AlienVault come alimentatore di minaccia esterno per ESA

Sommario

Introduzione

In questo documento viene descritto come configurare i feed delle minacce esterne da una sorgente AlienVault e come utilizzarli nell'ESA.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Email Security Appliance
- Python 3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il framework External Threat Feeds (ETF) consente al gateway e-mail di acquisire informazioni sulle minacce esterne condivise in formato STIX tramite il protocollo TAXII. Sfruttando questa capacità, le organizzazioni possono:

- Prendere una posizione proattiva contro le minacce informatiche come malware, ransomware, phishing e attacchi mirati.
- Sottoscrizione di fonti di informazioni sulle minacce locali e di terze parti.
- Migliorare l'efficacia complessiva del gateway di posta elettronica.

Che cos'è STIXX/TAXII?

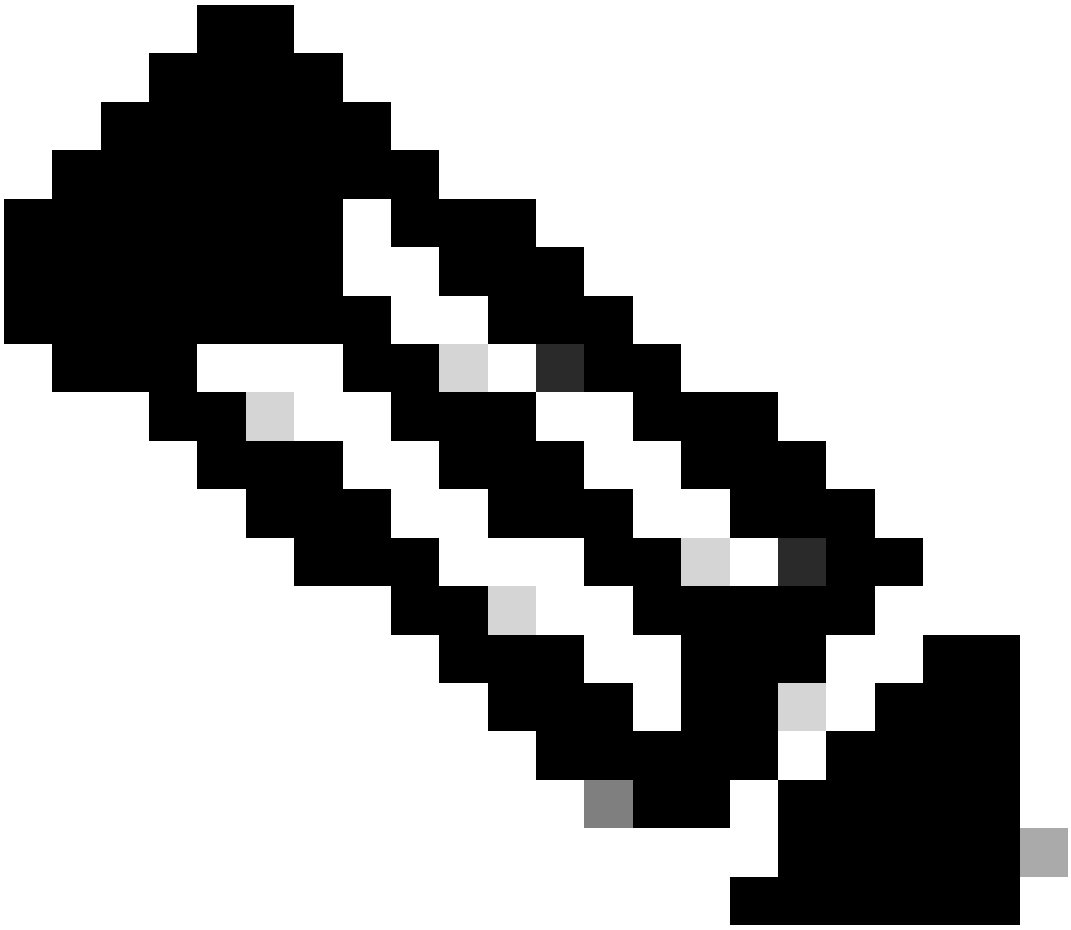
STIX (Structured Threat Information Expression, Espressione informazioni sulle minacce strutturate)

STIX è un formato standard utilizzato per descrivere in modo strutturato e leggibile da una macchina le funzionalità CTI (Cyber Threat Intelligence), inclusi indicatori, tattiche, tecniche, malware e attori di minacce. Un feed STIX include in genere degli indicatori, ovvero dei modelli che aiutano a rilevare attività informatiche sospette o dannose.

TAXII (Trusted Automated Exchange of Intelligence Information, Scambio automatizzato di informazioni di intelligence di fiducia)

TAXII è un protocollo utilizzato per lo scambio di dati STIX tra sistemi in modo sicuro e

automatico. Definisce il modo in cui i sistemi, i prodotti o le organizzazioni scambiano informazioni sulle minacce informatiche tramite servizi dedicati (server TAXII).



Nota: AsyncOS 16.0 supporta le versioni STIX/TAXII: STIX 1.1.1 e 1.2, con TAXII 1.1.

Origini feed

Le appliance di sicurezza e-mail possono utilizzare feed di intelligence provenienti da diverse fonti, inclusi repository pubblici, fornitori commerciali e i propri server privati all'interno dell'organizzazione.

Per garantire la compatibilità, tutte le fonti devono utilizzare gli standard STIX/TAXII, che consentono la condivisione strutturata e automatizzata dei dati sulle minacce.

Libreria Cabby

La libreria Cabby Python è uno strumento utile per la connessione ai server TAXII, l'individuazione delle collezioni STIX e il polling dei dati delle minacce. È un ottimo modo per verificare e convalidare il corretto funzionamento di un'origine feed e restituire i dati come previsto prima di integrarla in Email Security Appliance.

Installazione della libreria di file CAB

Per installare la libreria Cabby, è necessario verificare che nel computer locale sia installato Python pip.

Una volta installato python pip, è sufficiente eseguire questo comando per installare la libreria cabby.

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

Al termine dell'installazione della libreria a tassì, è possibile verificare che siano disponibili i comandi taxii-collection e taxii-poll.

```
(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 - Impulsi e feed

Per iniziare a scoprire le informazioni di AlienVault, creare prima un account sul sito AlienVault, quindi iniziare a cercare le informazioni desiderate.

In AlienVault, i feed e gli impulsi sono correlati ma non sono gli stessi:

Pulse

Gli impulsi sono stimolati dalla minaccia con indicatori raggruppati + contesto (leggibile dall'uomo).

- Un Pulse è una raccolta di indicatori di minaccia (IOC) raggruppati intorno a una minaccia o campagna specifica.
- Creato dalla comunità o dai provider per descrivere cose come malware, phishing, ransomware.
- Ogni impulso include contesto come descrizione della minaccia, indicatori associati (IP, dominio, hash del file e così via), tag e riferimenti.
- Gli impulsi sono leggibili e strutturati in modo da poter essere facilmente compresi e condivisi.

Si pensi a un impulso come a un report di minaccia con IOC e metadati raggruppati.

Feed

Gli alimentatori sono flussi automatizzati di indicatori provenienti da impulsi multipli (leggibili da macchina).

- I feed sono un flusso di indicatori grezzi (COI) estratti da uno o più impulsi, di solito in modo automatico.
- Sono in genere utilizzati dagli strumenti di sicurezza per acquisire gli indicatori in massa, tramite formati quali STIX/TAXII, CSV o JSON.
- I feed sono incentrati sul computer e vengono utilizzati per l'automazione e l'integrazione con SIEM, firewall e gateway di posta elettronica.

Un feed è più sul meccanismo di consegna, mentre un impulso è il contenuto e il contesto della minaccia.

Di solito si studia l'alimentazione, che è fatta di indicatori estratti dagli impulsi.

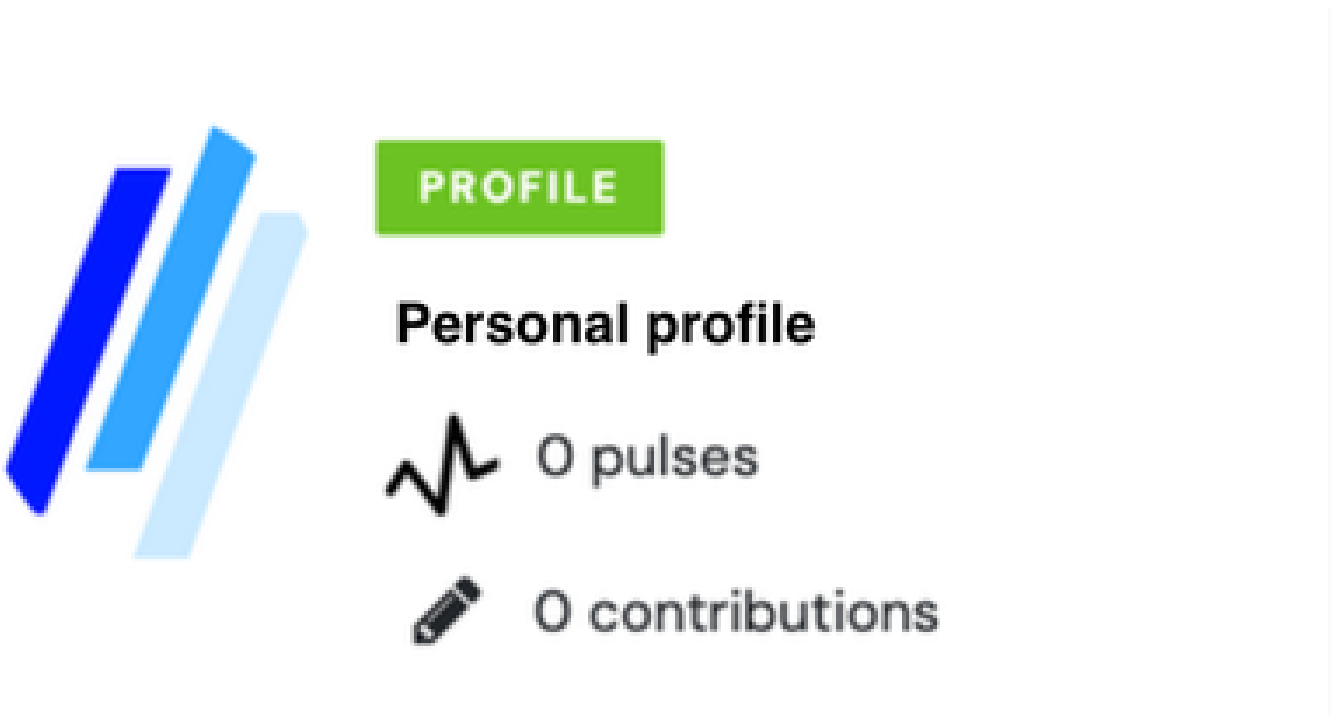
Avvia raccolta di polling

Polling dal proprio profilo

Dopo aver ottenuto l'account AlienVault, è possibile iniziare a usare i comandi taxii-collection e taxii-poll.

Di seguito viene indicato come utilizzare i comandi per questo scenario:

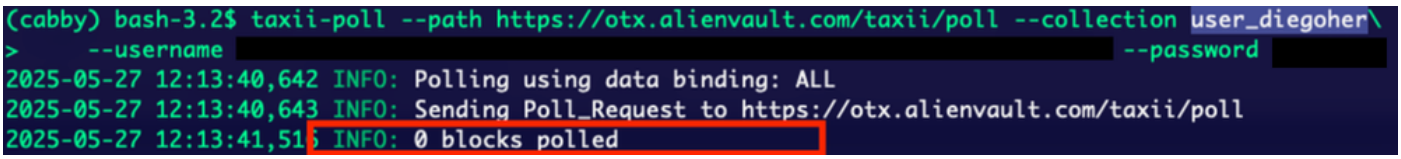
In questo caso, all'interno del profilo AlienVault non sono disponibili impulsi, ma come prova è possibile eseguire il polling di una raccolta dal profilo utilizzando il comando taxii-poll:



profilo personale alienvault

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

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

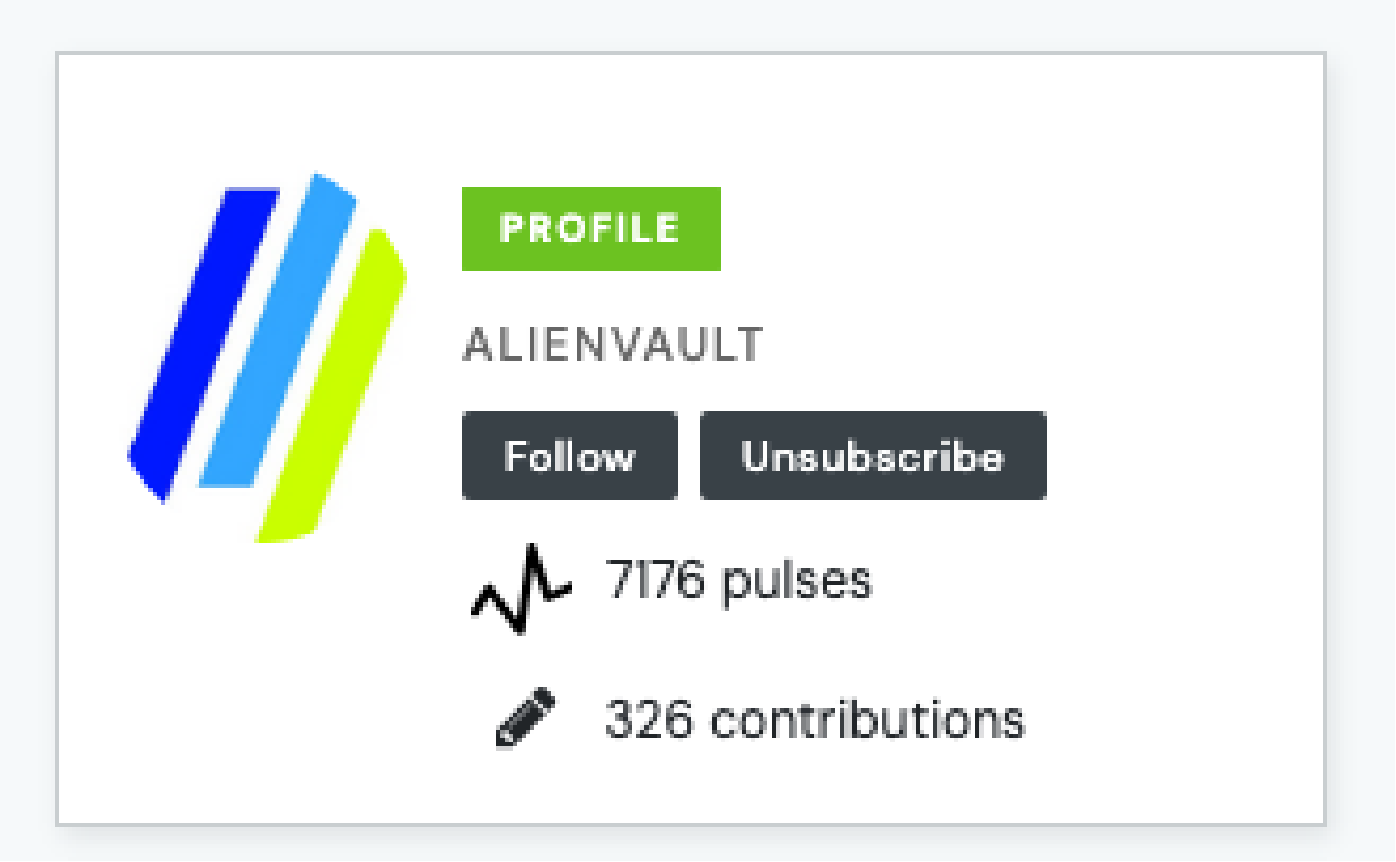


poll profilo personale

Come si può vedere, non sono stati eseguiti polling dei blocchi perché non sono disponibili informazioni nel profilo AlienVault.

Polling da profili AlienVault

Una volta scoperti i profili all'interno di AlienVault, alcuni di essi sono dotati di impulsi. Nell'esempio viene utilizzato il profilo AlienVault.



profilo di alienvault

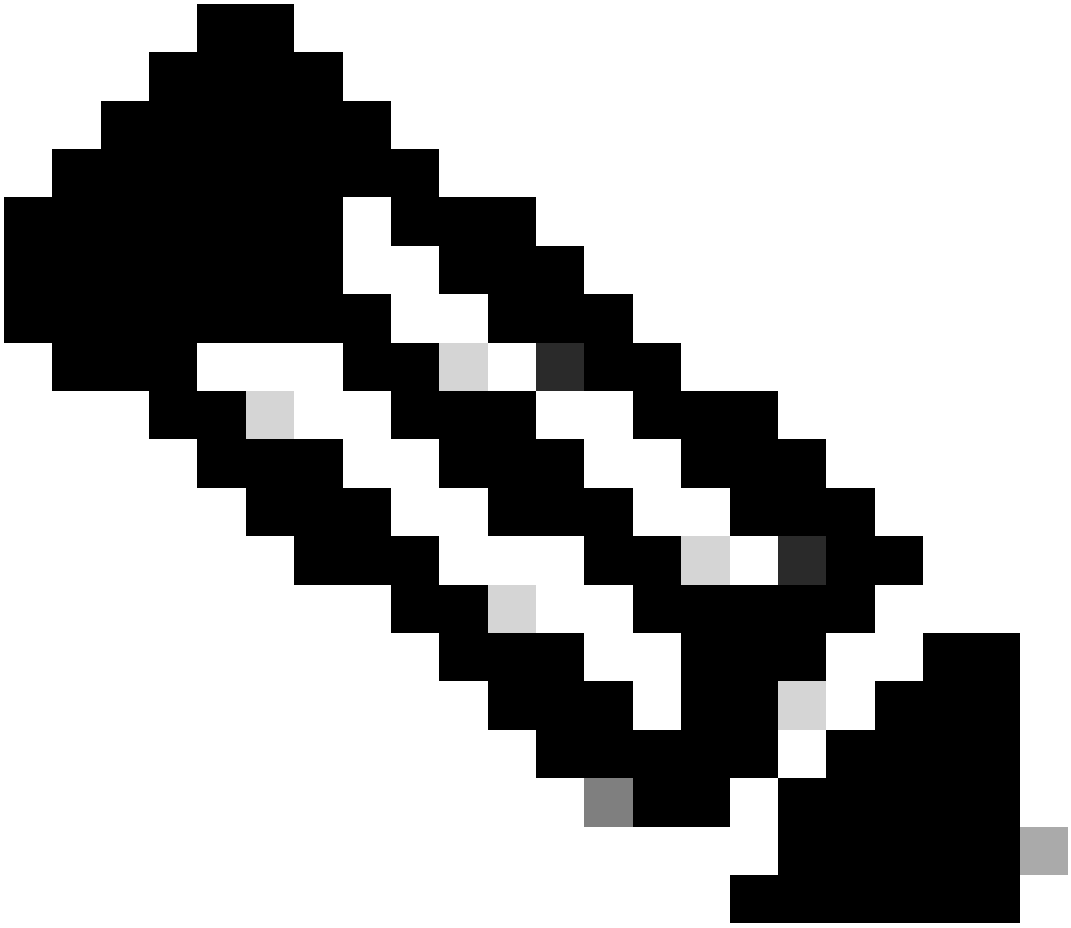
Quando si esegue il polling con il comando taxii-poll, viene immediatamente avviato il recupero di tutte le informazioni dal profilo.

```
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:/
```

sondaggio alienvault

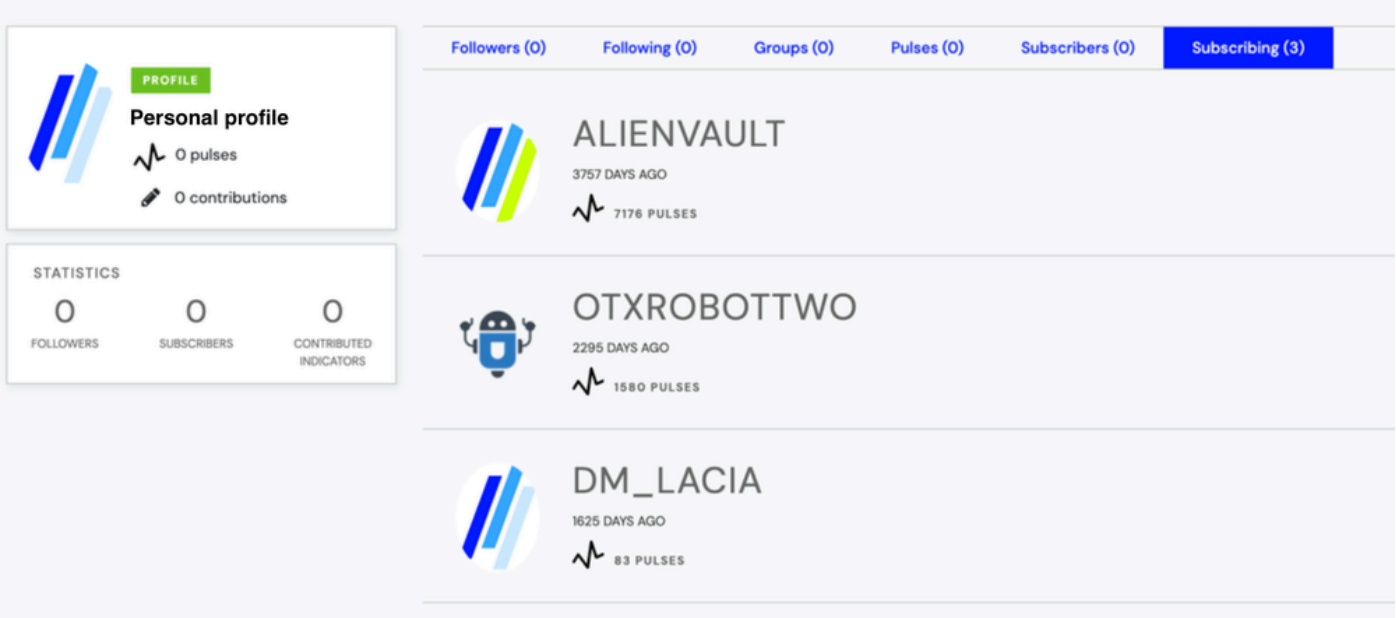
Come illustrato, il processo inizia a recuperare le informazioni.



Nota: Per sapere qual è il tuo nome utente e la tua password, controlla questo collegamento https://otx.alienvault.com/api

Abbonamenti alla raccolta di profili AlienVault

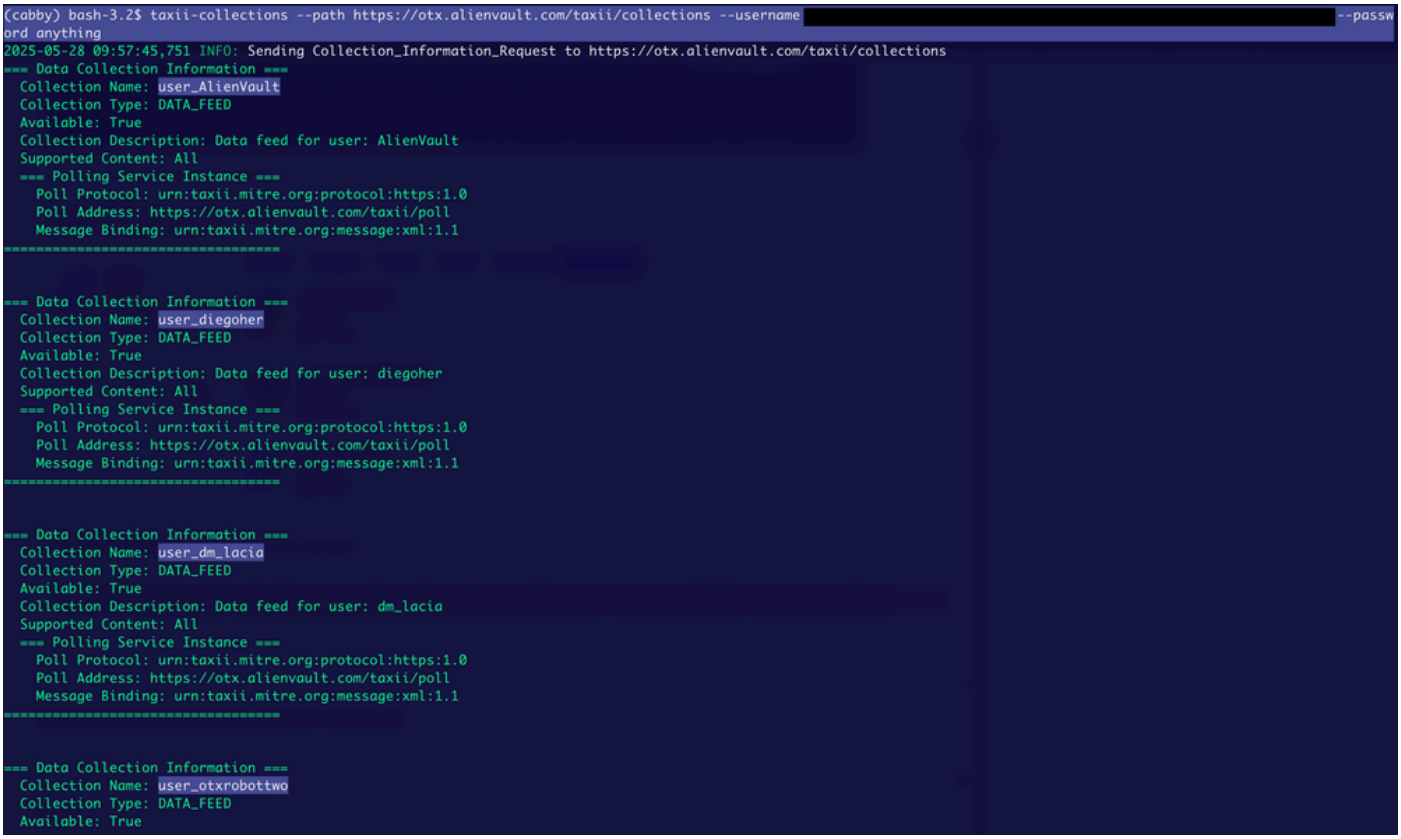
A titolo di prova, l'utente ha sottoscritto 3 profili.



sottoscrizioni profilo personale

È possibile utilizzare il comando taxii-collection per recuperare tali sottoscrizioni.

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



raccolte di profili personali

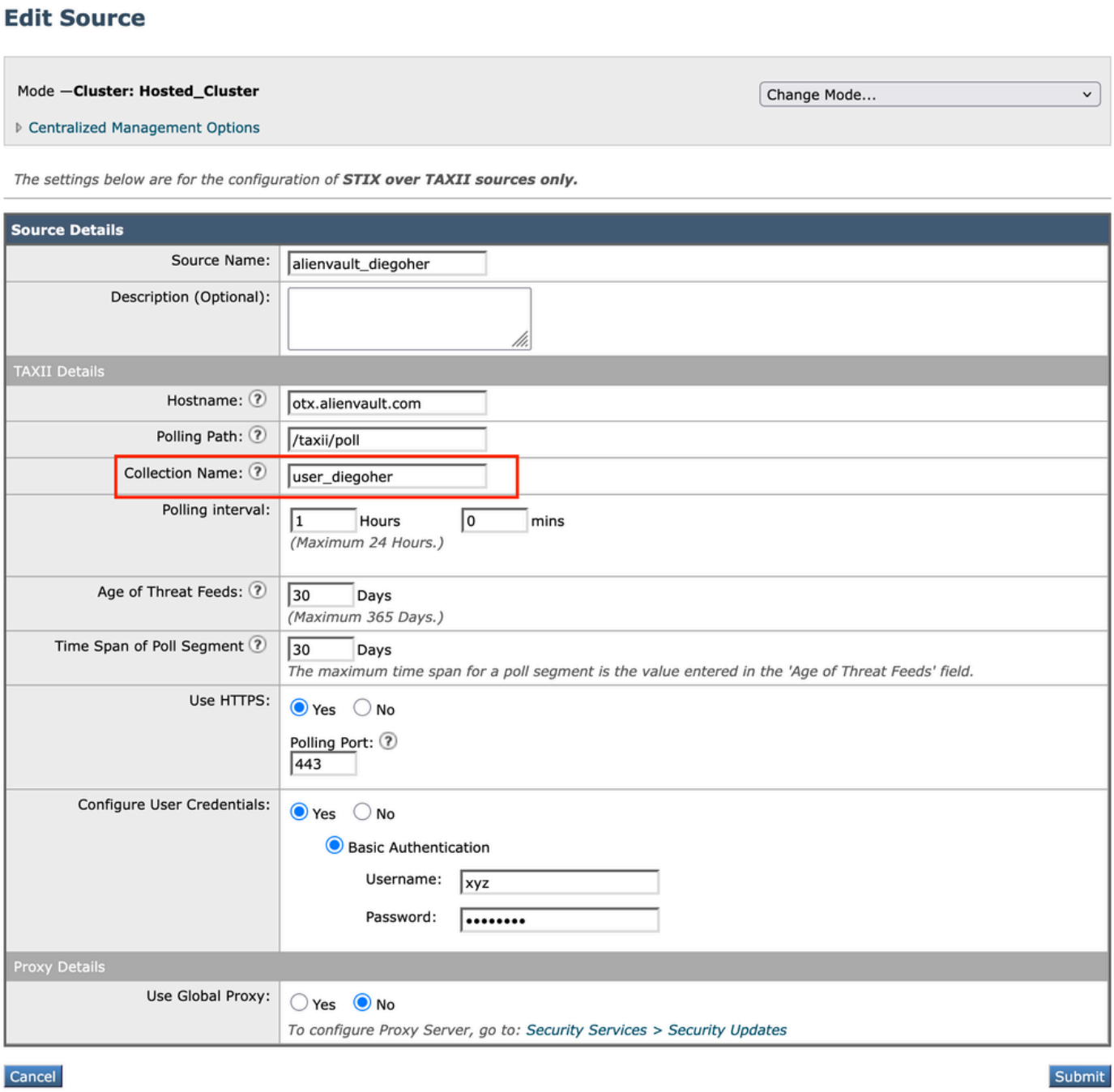
È possibile confermare che il comando taxii-collection funziona se il nome della raccolta è uguale

a quello sottoscritto.

Aggiunta di fonti a ESA

Aggiunta di un'origine senza feed

1. Passare a Mail Policies > External Threat Feeds Manager (Policy di posta > Gestione feed minacce esterne).
2. Passare alla modalità cluster.
3. Fare clic su Aggiungi origine.
4. Nome host: otx.alienvault.com
5. Percorso di polling: /taxi/poll
6. Nome raccolta: user_<nome_utente_AlienVault>
7. Port: 443
8. Configurare le credenziali utente: Quello fornito da AlienVault.
9. Fare clic su Sottometti > Conferma modifiche.



origine personale

Origine polling senza feed

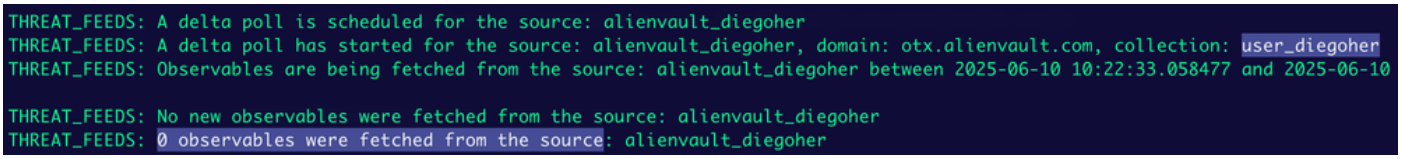
In Gestione feed minacce esterne, dopo l'aggiunta dell'origine, l'origine appena aggiunta diventa visibile.

feed personale

Una volta aggiunto, fare clic su Raccogli ora.

Verifica

Accedere all'ESA tramite la CLI ed esaminare i log dei feed delle minacce per verificare le informazioni.

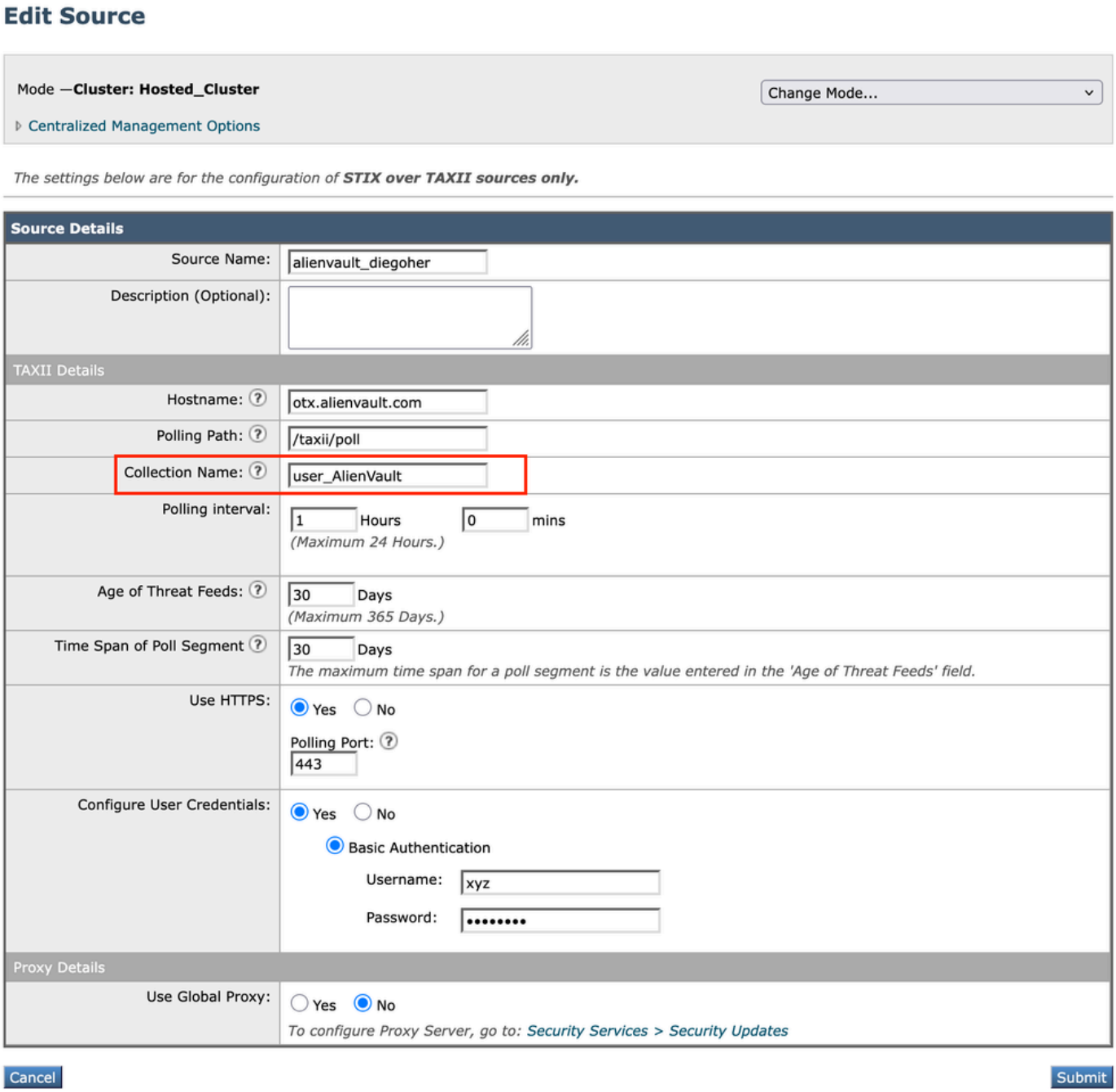


Sondaggio personale ETF

Come mostrato nell'immagine, è possibile notare che 0 osservabili sono stati recuperati e questo è previsto perché non ci sono feed nel profilo mostrato.

Aggiunta di un'origine con feed

1. Passare a Mail Policies > External Threat Feeds Manager (Policy di posta > Gestione feed minacce esterne).
2. Passare alla modalità cluster.
3. Fare clic su Aggiungi origine.
4. Nome host: otx.alienvault.com
5. Percorso di polling: /taxi/poll
6. Nome raccolta: user_AlienVault
7. Port: 443
8. Configurare le credenziali utente: Quello fornito da AlienVault.
9. Fare clic su Sottometti > Conferma modifiche.



origine alienvault

Origine polling con feed

In Gestione feed minacce esterne, dopo l'aggiunta dell'origine, l'origine appena aggiunta diventa visibile.

feed alienvault

Una volta aggiunto, fare clic su Raccogli ora.

Verifica

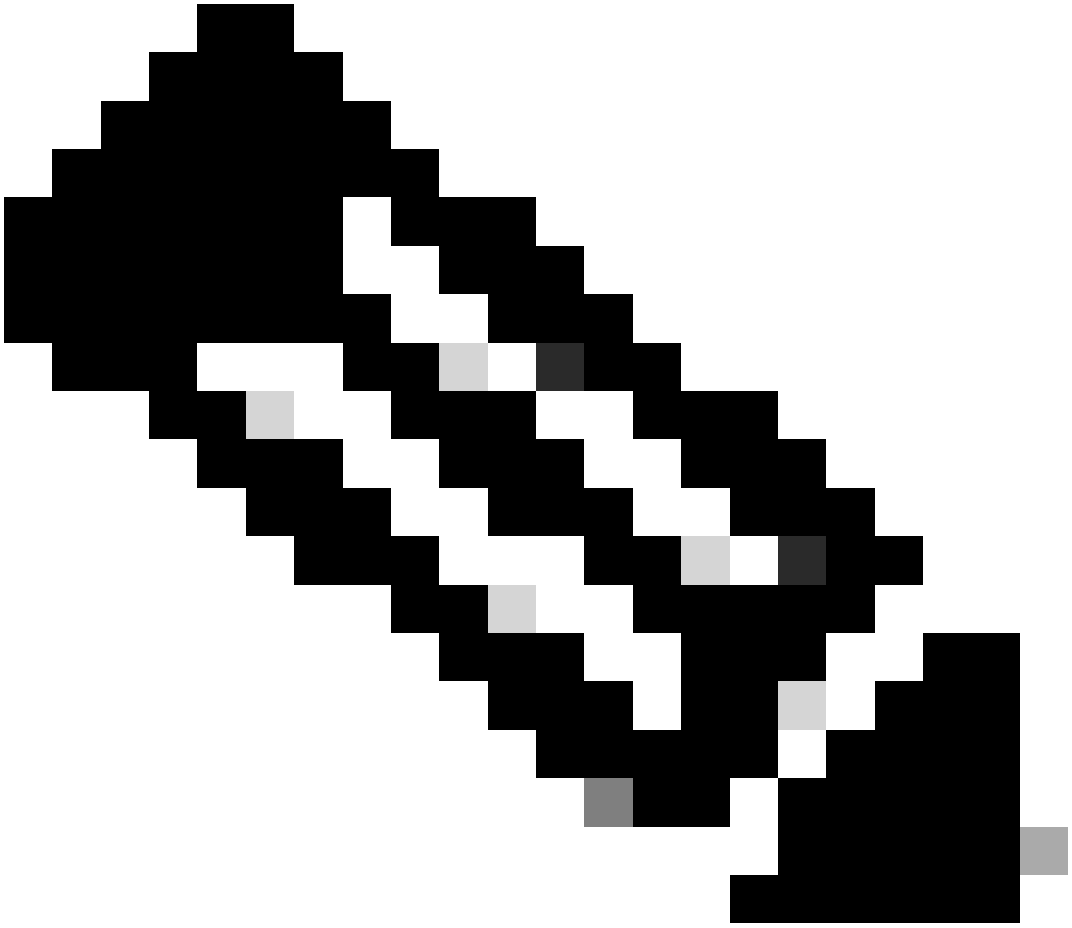
Accedere all'ESA tramite la CLI ed esaminare i log dei feed delle minacce per verificare le informazioni.

```
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
```

polling del feed alienvault

Come mostrato nell'immagine, si può vedere che diversi osservatori sono stati catturati.



Nota: Se vengono aggiunti nuovi feed alla raccolta configurata, l'ESA esegue automaticamente il polling dell'origine e i nuovi oggetti osservabili vengono recuperati.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).