Konfigurieren von AlienVault als externer Bedrohungs-Feed für die ESA

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Was ist STIXX/TAXII?
  - STIX (Structured Threat Information Expression)
  - TAXII (Trusted Automated Exchange of Intelligence Information)
- Futterquellen
- Cabby-Bibliothek
  - Installation der Kabinenbibliothek
- AlienVault - Pulse und Feeds
  - Pulse
  - Feeds
- Polling-Auflistungen starten
  - Polling aus eigenem Profil
  - Polling von AlienVault-Profilen
  - Abonnements für die AlienVault-Profilerfassung
- Hinzufügen von Quellen zur ESA
  - Hinzufügen einer Quelle ohne Feeds
  - Polling-Quelle ohne Feeds
  - Überprüfung
  - Hinzufügen von Quelle mit Feeds
  - Polling-Quelle mit Feeds
  - Überprüfung

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration externer Bedrohungs-Feeds von einer AlienVault-Quelle und deren Verwendung innerhalb der ESA beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Secure Email Gateway (SEG/ESA) AsyncOS 16.0.2
- Linux-Kommandozeile
- Python3-Pipeline
- AlienVault-Konto

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- E-Mail Security Appliance
- Python 3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Das ETF-Framework (External Threat Feeds) ermöglicht dem E-Mail-Gateway die Erfassung externer Bedrohungsinformationen, die über das TAXII-Protokoll im STIX-Format ausgetauscht werden. Durch die Nutzung dieser Funktion ergeben sich folgende Möglichkeiten:

- Gehen Sie proaktiv gegen Cyber-Bedrohungen wie Malware, Ransomware, Phishing und zielgerichtete Angriffe vor.
- Abonnieren Sie lokale Threat-Intelligence und Threat-Intelligence von Drittanbietern.
- Erhöhen Sie die Effektivität des E-Mail-Gateways.

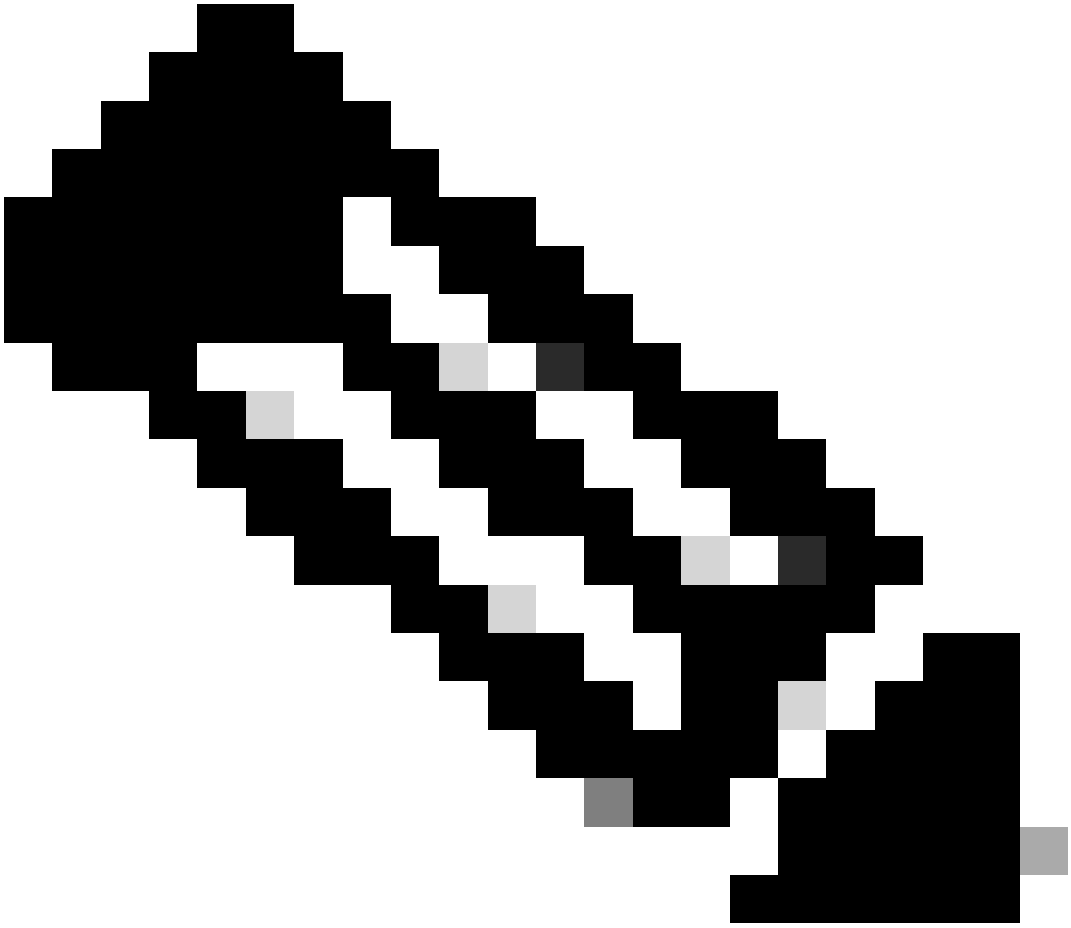
Was ist STIXX/TAXII?

STIX (Structured Threat Information Expression)

STIX ist ein standardisiertes Format zur strukturierten und maschinenlesbaren Beschreibung von Cyber Threat Intelligence (CTI), einschließlich Indikatoren, Taktiken, Techniken, Malware und Angreifern. Ein STIX-Feed umfasst in der Regel Indikatoren - Muster, die dabei helfen, verdächtige oder schädliche Cyber-Aktivitäten zu erkennen.

TAXII (Trusted Automated Exchange of Intelligence Information)

TAXII ist ein Protokoll für den sicheren und automatischen Austausch von STIX-Daten zwischen Systemen. Definiert, wie Informationen zu Cyberbedrohungen zwischen Systemen, Produkten oder Organisationen über dedizierte Services (TAXII-Server) ausgetauscht werden.



Hinweis: AsyncOS 16.0 unterstützt STIX/TAXII Versionen: STIX 1.1.1 und 1.2, mit TAXII 1.1.

Futterquellen

E-Mail Security Appliances können Feeds mit Bedrohungsinformationen aus verschiedenen Quellen nutzen, darunter öffentliche Repositories, kommerzielle Anbieter und ihre eigenen privaten Server in Ihrem Unternehmen.

Zur Gewährleistung der Kompatibilität müssen alle Quellen die STIX/TAXII-Standards verwenden, die eine strukturierte, automatisierte Freigabe von Bedrohungsdaten ermöglichen.

Cabby-Bibliothek

Die Cabby Python-Bibliothek ist ein nützliches Tool für die Verbindung mit TAXII-Servern, die Entdeckung von STIX-Sammlungen und das Polling von Bedrohungsdaten. Dies ist eine hervorragende Möglichkeit, vor der Integration in Ihre E-Mail Security Appliance zu testen, ob eine Feed-Quelle ordnungsgemäß funktioniert, und die Daten wie erwartet zurückzugeben.

Installation der Kabinenbibliothek

Um die Cabby-Bibliothek zu installieren, müssen Sie sicherstellen, dass auf Ihrem lokalen Rechner Python pip installiert ist.

Sobald python pip installiert ist, müssen Sie nur noch diesen Befehl ausführen, um die Cabby-Bibliothek zu installieren.

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

Nachdem die Installation der Kabinenbibliothek abgeschlossen ist, können Sie überprüfen, ob die Befehle taxii-collections und taxii-poll jetzt verfügbar sind.

```
(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 - Pulse und Feeds

Um AlienVault-Informationen zu erkennen, erstellen Sie zunächst ein Konto auf der AlienVault-Website, und suchen Sie dann nach den gewünschten Informationen.

In AlienVault sind Feeds und Impulse verwandt, aber nicht identisch:

Pulse

Pulse werden mithilfe von gruppierten Indikatoren und Kontext (für Menschen lesbar) als Bedrohungsinformationen behandelt.

- Ein Pulse ist eine Zusammenstellung von Bedrohungsindikatoren (IOCs), die sich um eine bestimmte Bedrohung oder Kampagne gruppieren.
- Erstellt von der Community oder Anbietern, um Dinge wie Malware, Phishing, Ransomware zu beschreiben.
- Jeder Impuls umfasst Kontext wie Bedrohungsbeschreibung, zugehörige Indikatoren (IP, Domäne, Datei-Hash usw.), Tags und Verweise.
- Pulse sind für Menschen lesbar und so strukturiert, dass sie leicht verstanden und geteilt werden können.

Stellen Sie sich einen Impuls als Bedrohungsbericht mit gruppierten IOCs und Metadaten vor.

Feeds

Feeds sind automatisierte Anzeigeströme aus mehreren Impulsen (maschinenlesbar).

- Feeds sind ein Strom von unformatierten Indikatoren (IOCs), die aus einem oder mehreren Pulsen gezogen werden, in der Regel auf automatisierte Weise.
- Sie werden in der Regel von Sicherheitstools verwendet, um Indikatoren in großen Mengen über Formate wie STIX/TAXII, CSV oder JSON aufzunehmen.
- Feeds sind auf bestimmte Systeme ausgerichtet und werden für die Automatisierung und Integration mit SIEMs, Firewalls und E-Mail-Gateways verwendet.

Bei einem Feed geht es mehr um den Bereitstellungsmechanismus, während ein Puls Inhalt und Kontext der Bedrohung ist.

Normalerweise werden Feeds abgefragt, und diese Feeds bestehen aus Indikatoren, die aus Pulsen extrahiert werden.

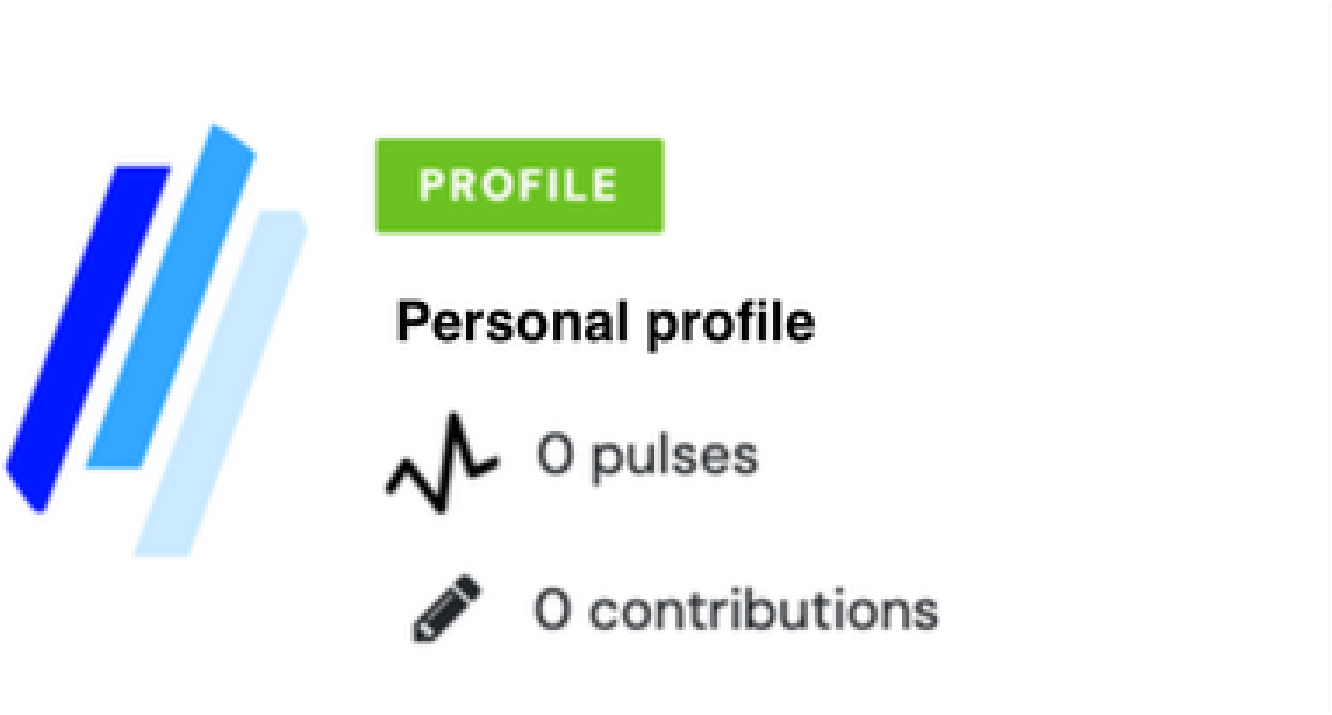
Polling-Auflistungen starten

Polling aus eigenem Profil

Sobald Sie Ihr AlienVault-Konto haben, können Sie mit den Befehlen taxii-collections und taxii-poll beginnen.

Hier erfahren Sie, wie Sie diese Befehle für diesen Anwendungsfall verwenden:

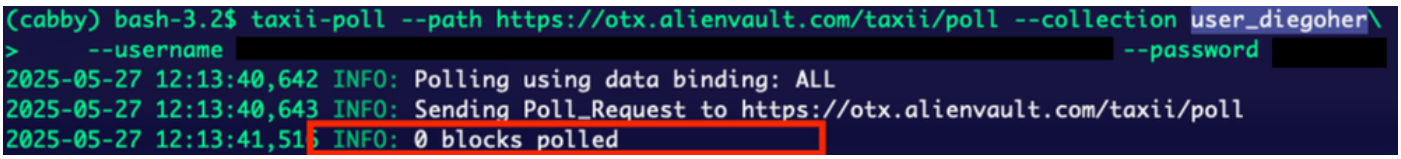
In diesem Fall sind im AlienVault-Profil keine Impulse verfügbar, aber Sie können als Test eine Sammlung Ihres Profils mit dem Befehl taxii-poll abfragen:



Personenprofil alienvault

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

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

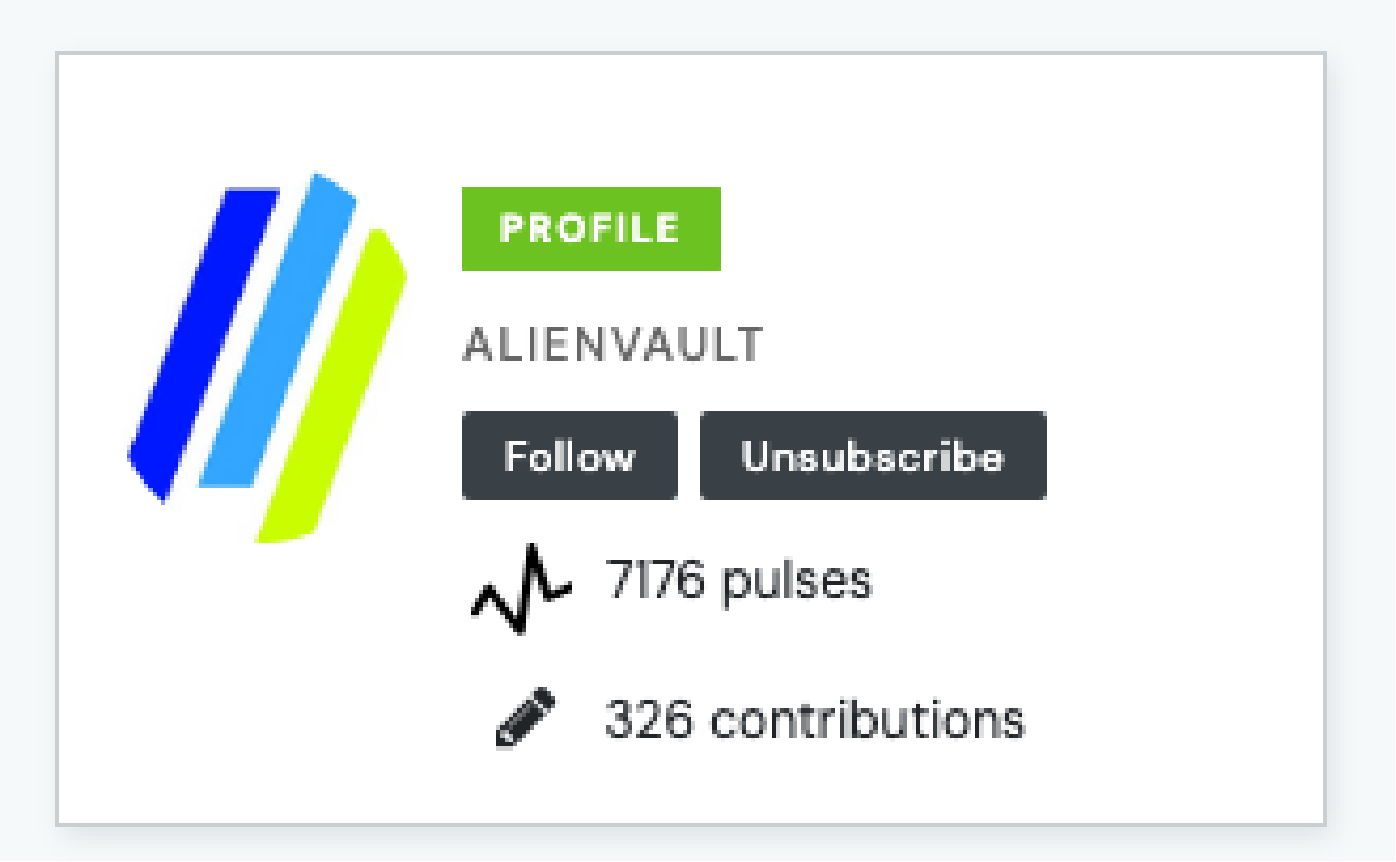


persönliches Profil der Umfrage

Wie Sie sehen, werden keine Blöcke abgefragt, da im AlienVault-Profil keine Informationen verfügbar sind.

Polling von AlienVault-Profilen

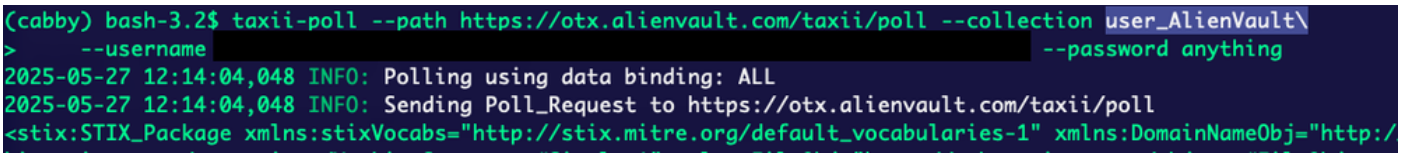
Sobald Profile in AlienVault entdeckt wurden, haben einige von ihnen Impulse. In diesem Beispiel wird das AlienVault-Profil verwendet.



Alienvault-Profil

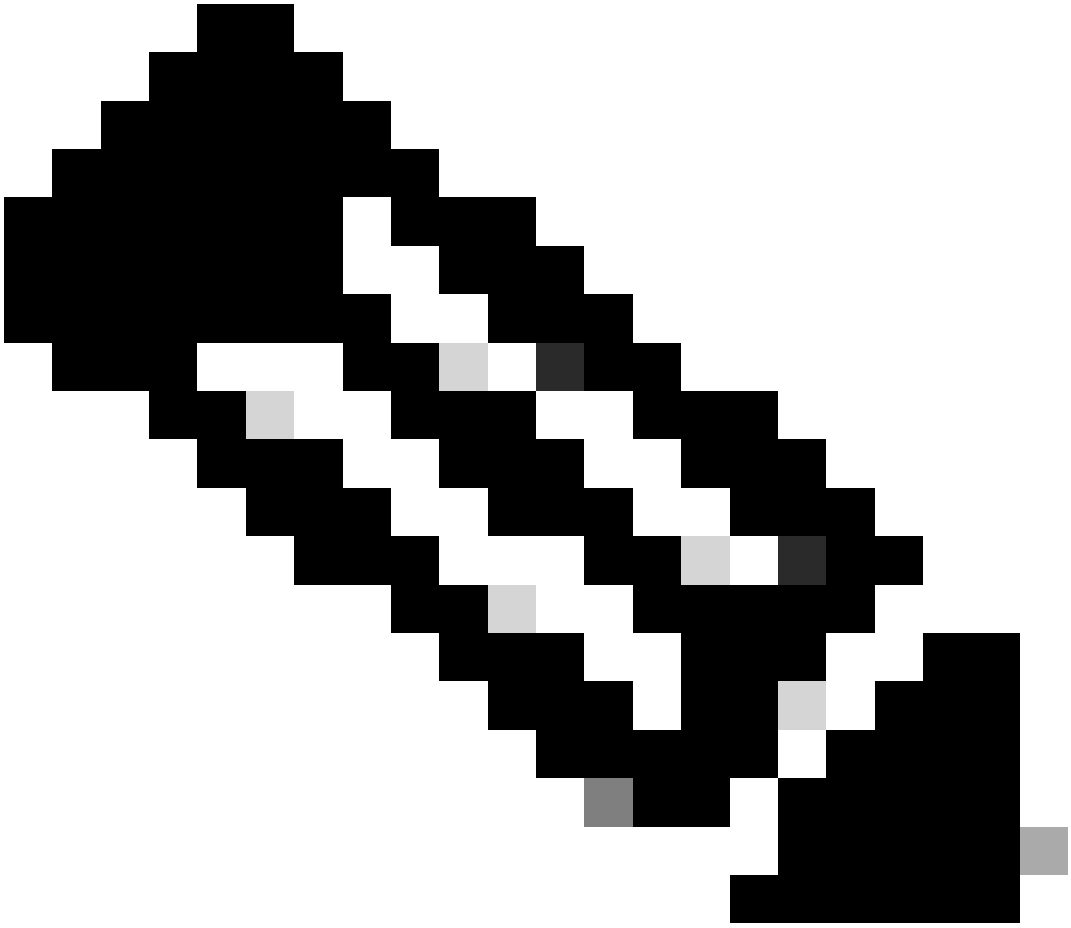
Wenn die Abfrage mit dem Befehl taxii-poll ausgeführt wird, werden sofort alle Informationen aus dem Profil abgerufen.

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



Alienvault-Umfrage

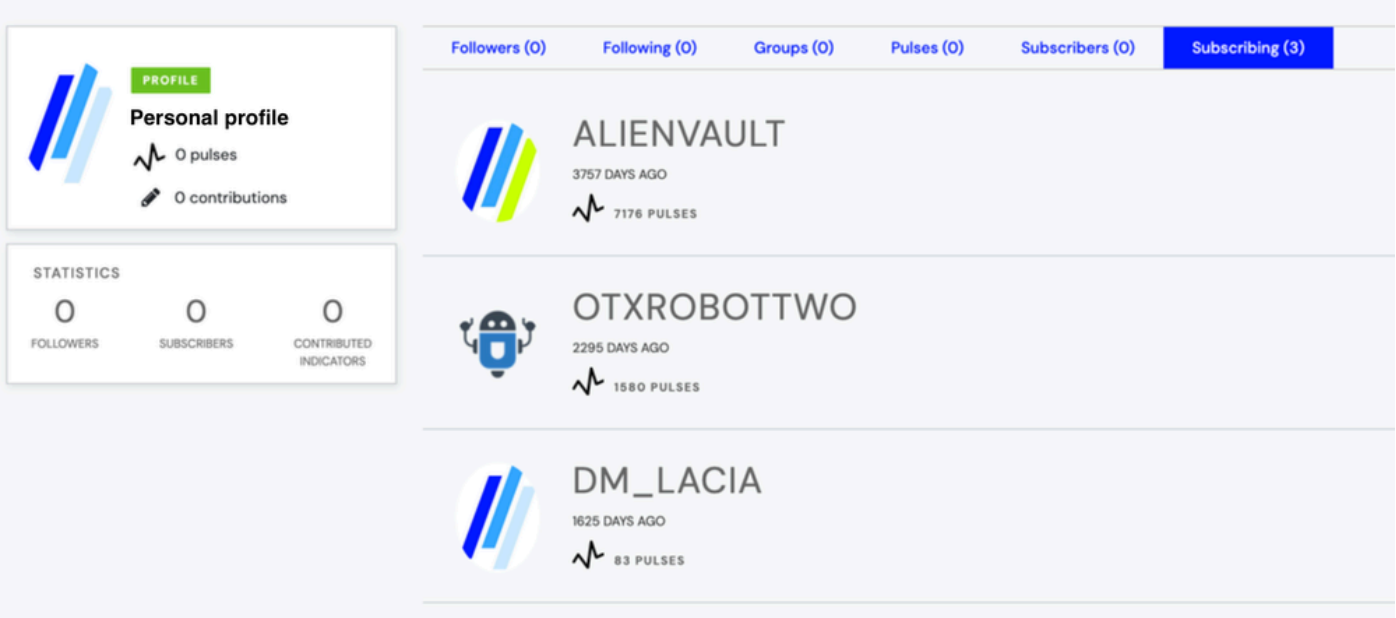
Wie dargestellt, beginnt der Prozess mit dem Abrufen der Informationen.



Anmerkung: Um herauszufinden, welcher Benutzername und welches Kennwort Sie haben, klicken Sie auf den folgenden Link: https://otx.alienvault.com/api

Abonnements für die AlienVault-Profilerfassung

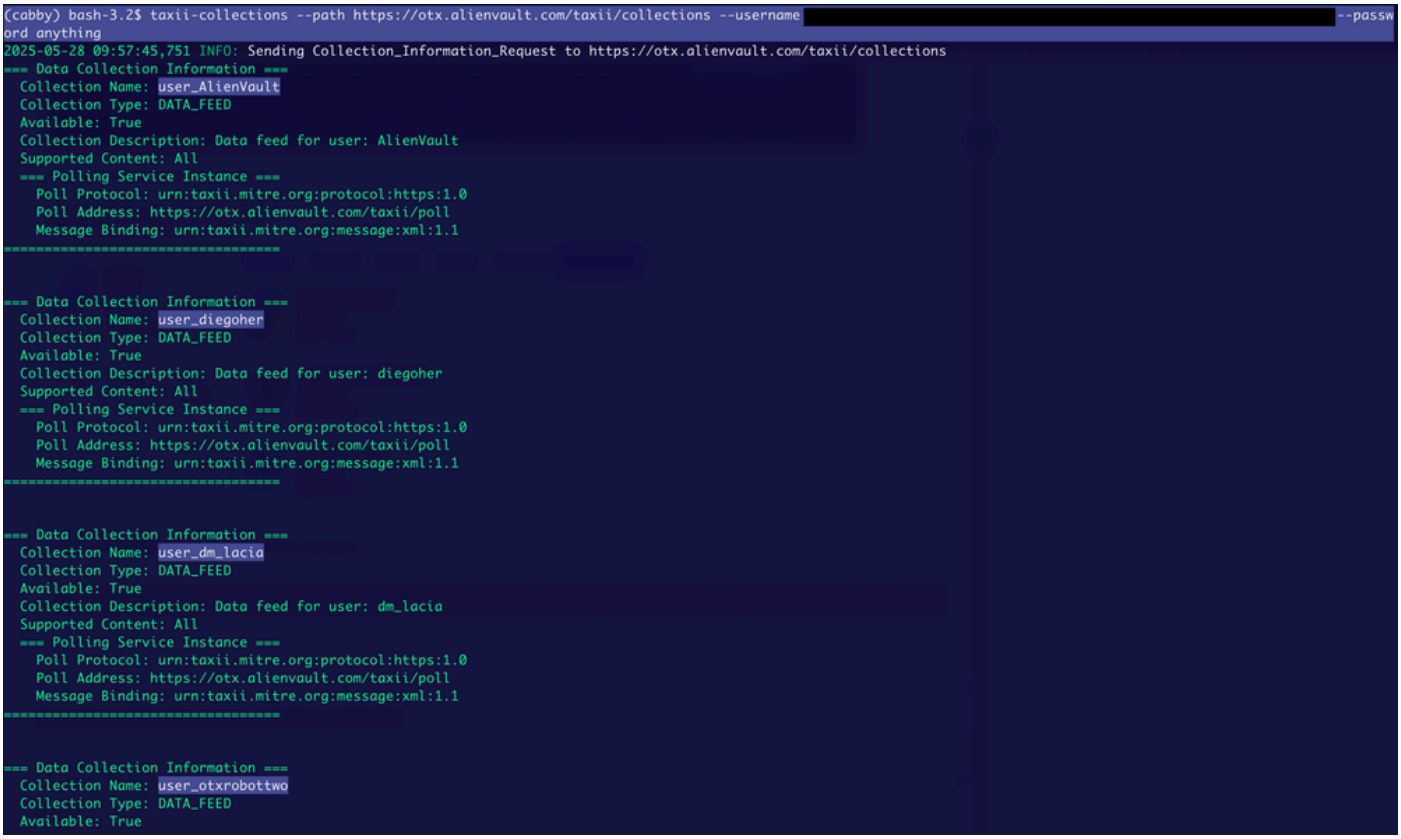
Als Test hat dieser Benutzer drei Profile abonniert.



Abonnements mit persönlichem Profil

Mit dem Befehl taxii-collections können Sie diese Abonnements abrufen.

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



persönliche Profilsammlungen

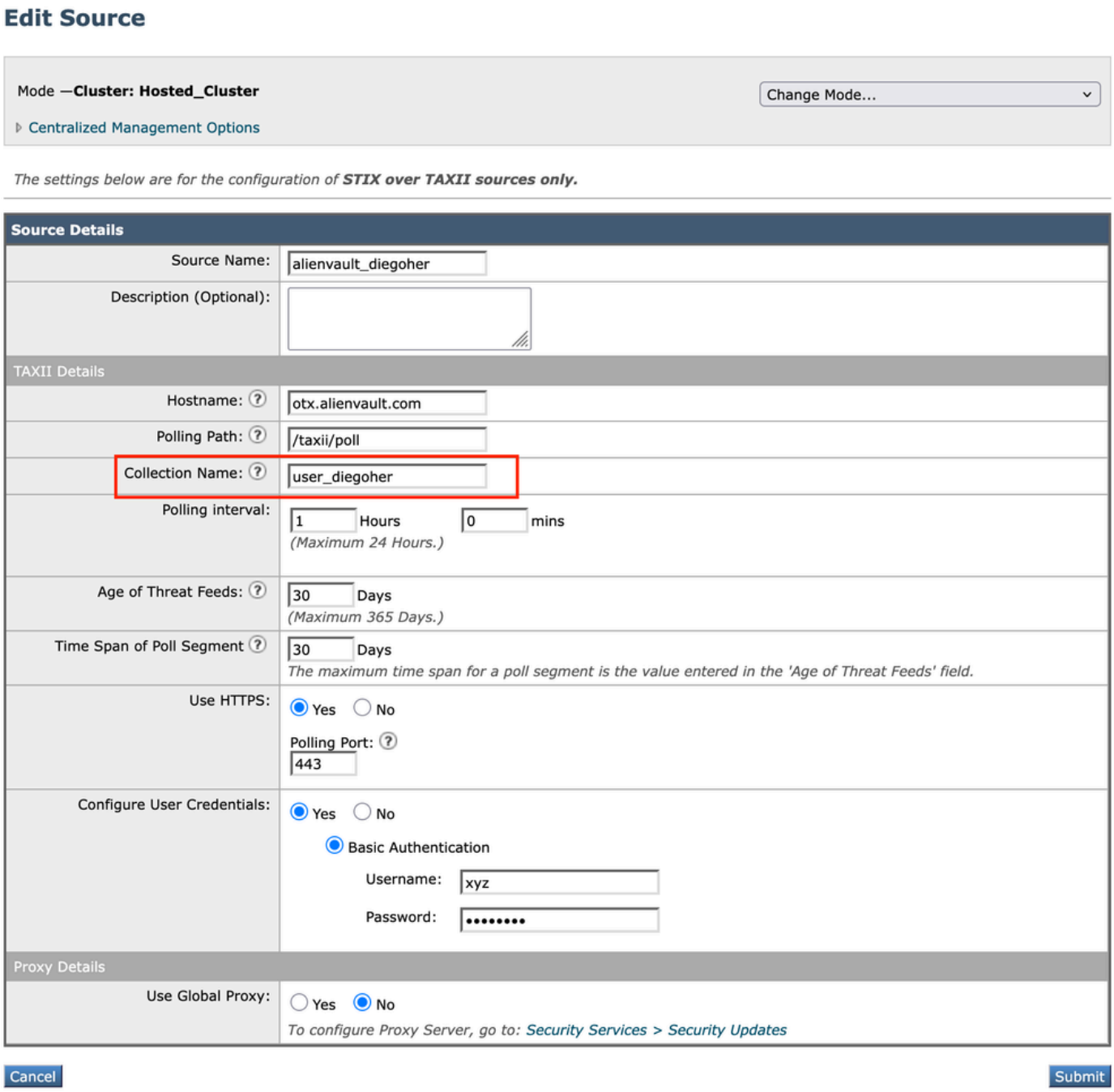
Sie können bestätigen, dass der Befehl taxii-collections funktioniert, wenn der Sammlungsname

mit dem Namen übereinstimmt, den Sie abonniert haben.

Hinzufügen von Quellen zur ESA

Hinzufügen einer Quelle ohne Feeds

1. Navigieren Sie zu Mail-Policys > External Threat Feeds Manager.
2. Wechseln Sie in den Clustermodus.
3. Klicken Sie auf Quelle hinzufügen.
4. Hostname: otx.alienvault.com
5. Polling-Pfad: /taxi/poll
6. Sammlungsname: user_<Ihr_AlienVault_Benutzername>
7. Anschluss: 443
8. Anmeldeinformationen des Benutzers konfigurieren: Die, die AlienVault Ihnen bereitgestellt hat.
9. Klicken Sie auf Senden > Änderungen bestätigen.



persönliche Quelle

Polling-Quelle ohne Feeds

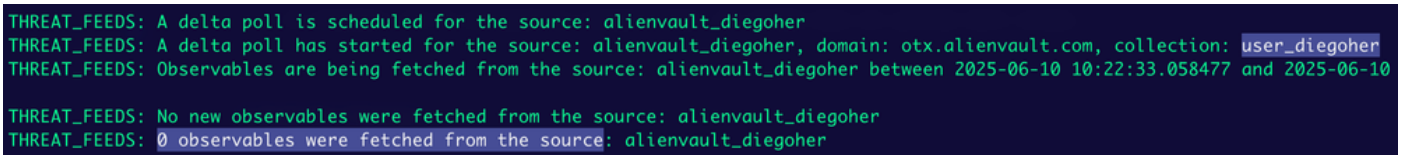
Nachdem die Quelle hinzugefügt wurde, wird die neu hinzugefügte Quelle im External Threat Feeds Manager angezeigt.

persönliches Futter

Klicken Sie nach dem Hinzufügen auf Jetzt abfragen.

Überprüfung

Melden Sie sich über die Kommandozeile bei der ESA an, und überprüfen Sie die Bedrohungs-Protokolle, um die Informationen zu überprüfen.

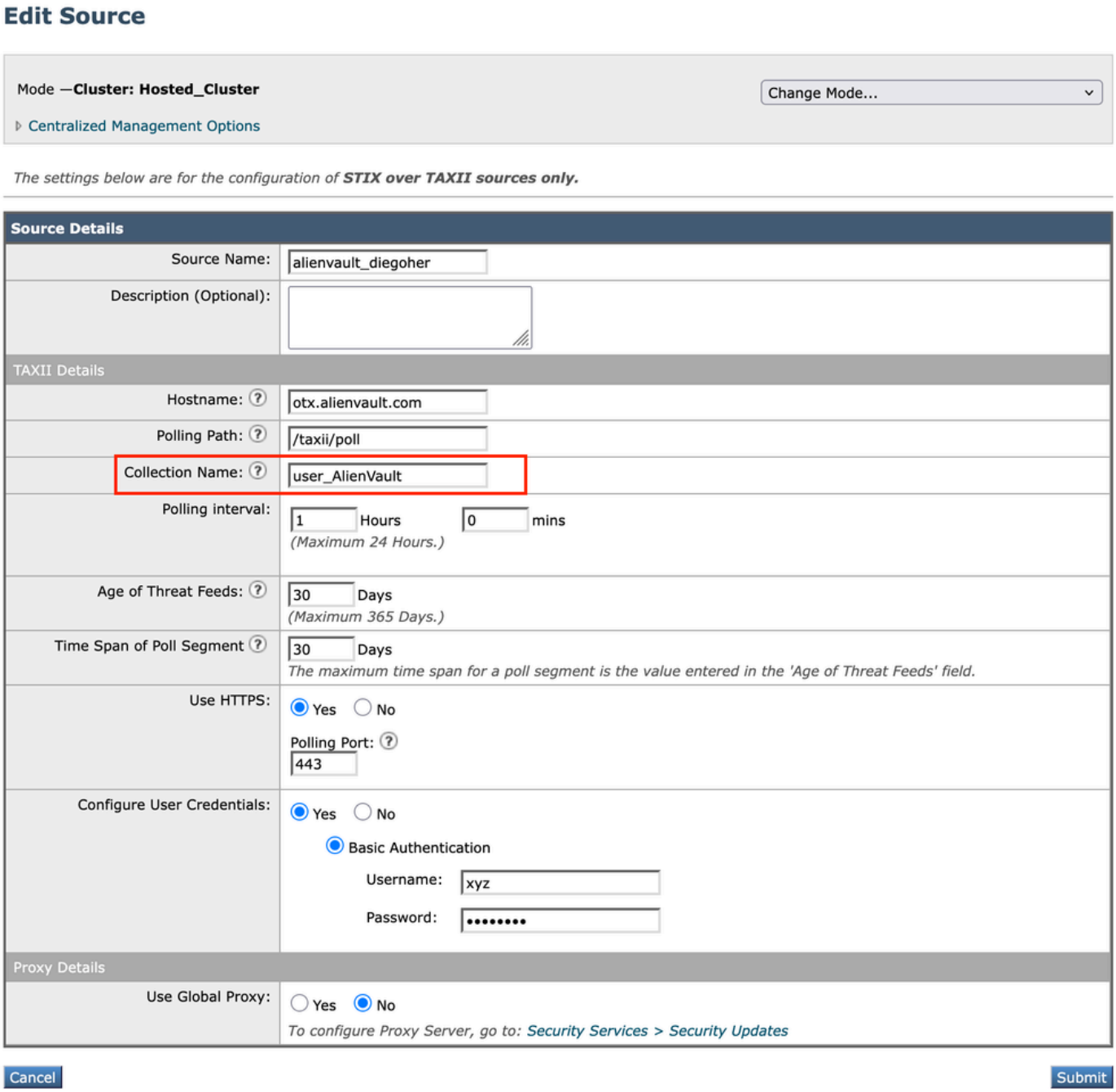


Persönliche ETF-Umfrage

Wie im Bild gezeigt, können Sie sehen, dass 0 Observables geholt wurden und dies erwartet wird, weil es keine Feeds in dem Profil gezeigt.

Hinzufügen von Quelle mit Feeds

1. Navigieren Sie zu Mail-Policys > External Threat Feeds Manager.
2. Wechseln Sie in den Clustermodus.
3. Klicken Sie auf Quelle hinzufügen.
4. Hostname: otx.alienvault.com
5. Polling-Pfad: /taxi/poll
6. Sammlungsname: user_AlienVault
7. Anschluss: 443
8. Anmeldeinformationen des Benutzers konfigurieren: Die, die AlienVault Ihnen bereitgestellt hat.
9. Klicken Sie auf Senden > Änderungen bestätigen.



Alienvault-Quelle

Polling-Quelle mit Feeds

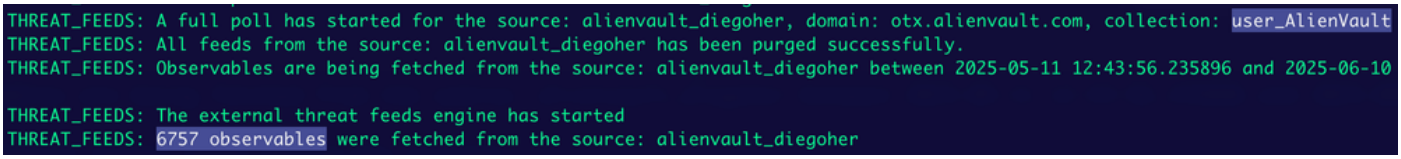
Nachdem die Quelle hinzugefügt wurde, wird die neu hinzugefügte Quelle im External Threat Feeds Manager angezeigt.

Alienvault-Feed

Klicken Sie nach dem Hinzufügen auf Jetzt abfragen.

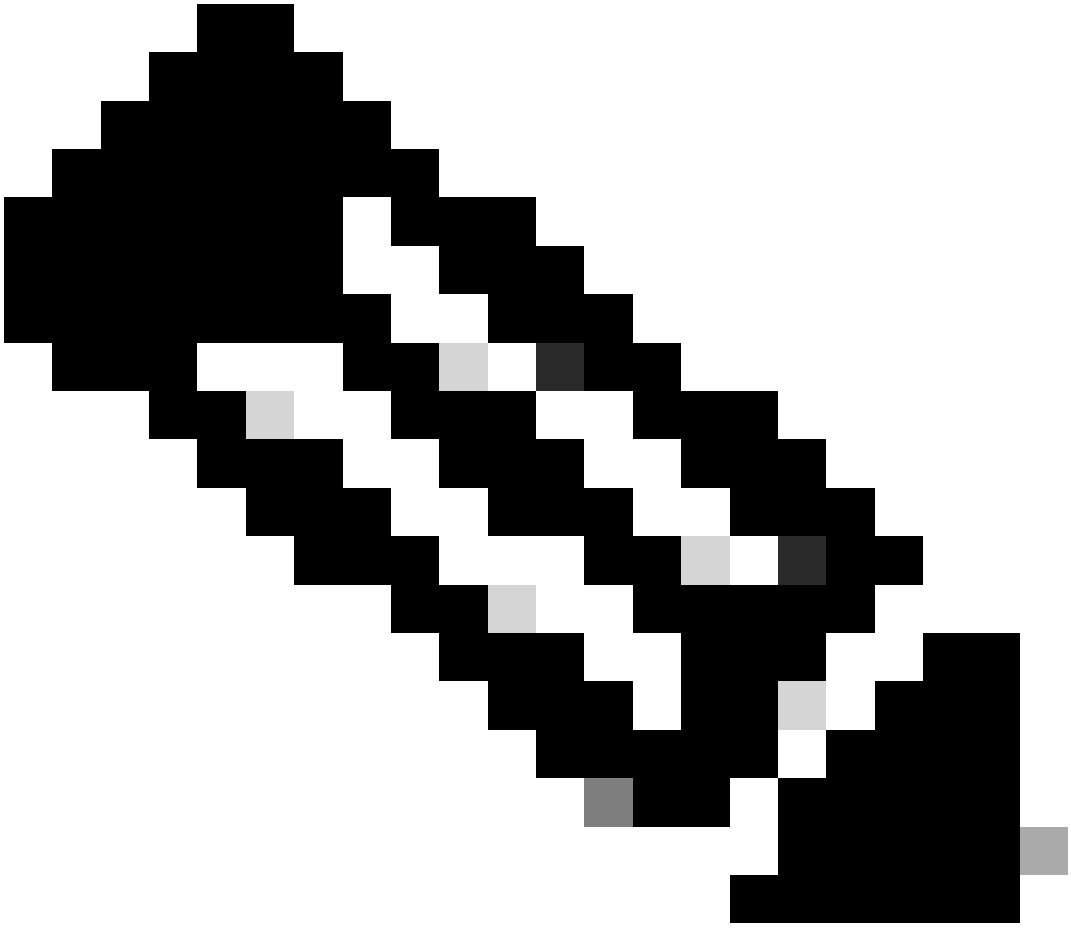
Überprüfung

Melden Sie sich über die Kommandozeile bei der ESA an, und überprüfen Sie die Bedrohungs-Protokolle, um die Informationen zu überprüfen.



Alienvault-Feed abfragen

Wie im Bild gezeigt, können Sie sehen, dass mehrere Observables geholt wurden.



Anmerkung: Wenn der konfigurierten Sammlung neue Feeds hinzugefügt werden, fragt die ESA automatisch die Quelle ab, und die neuen Observables werden abgerufen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.