Configuración de AlienVault como fuente de amenazas externas para ESA

Contenido

Introducción

Este documento describe los pasos para configurar las fuentes de amenazas externas de un origen de AlienVault y utilizarlas dentro del ESA.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Aplicación de seguridad de correo electrónico
- Python3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La estructura de fuentes de amenazas externas (ETF) permite al gateway de correo electrónico ingerir inteligencia de amenazas externas compartida en formato STIX mediante el protocolo TAXI. Al aprovechar esta capacidad, las organizaciones pueden:

- Adopte una postura proactiva frente a las amenazas cibernéticas, como el malware, el ransomware, la suplantación de identidad y los ataques selectivos.
- Suscríbase a fuentes de inteligencia de amenazas locales y de terceros.
- Mejore la eficacia general del gateway de correo electrónico.

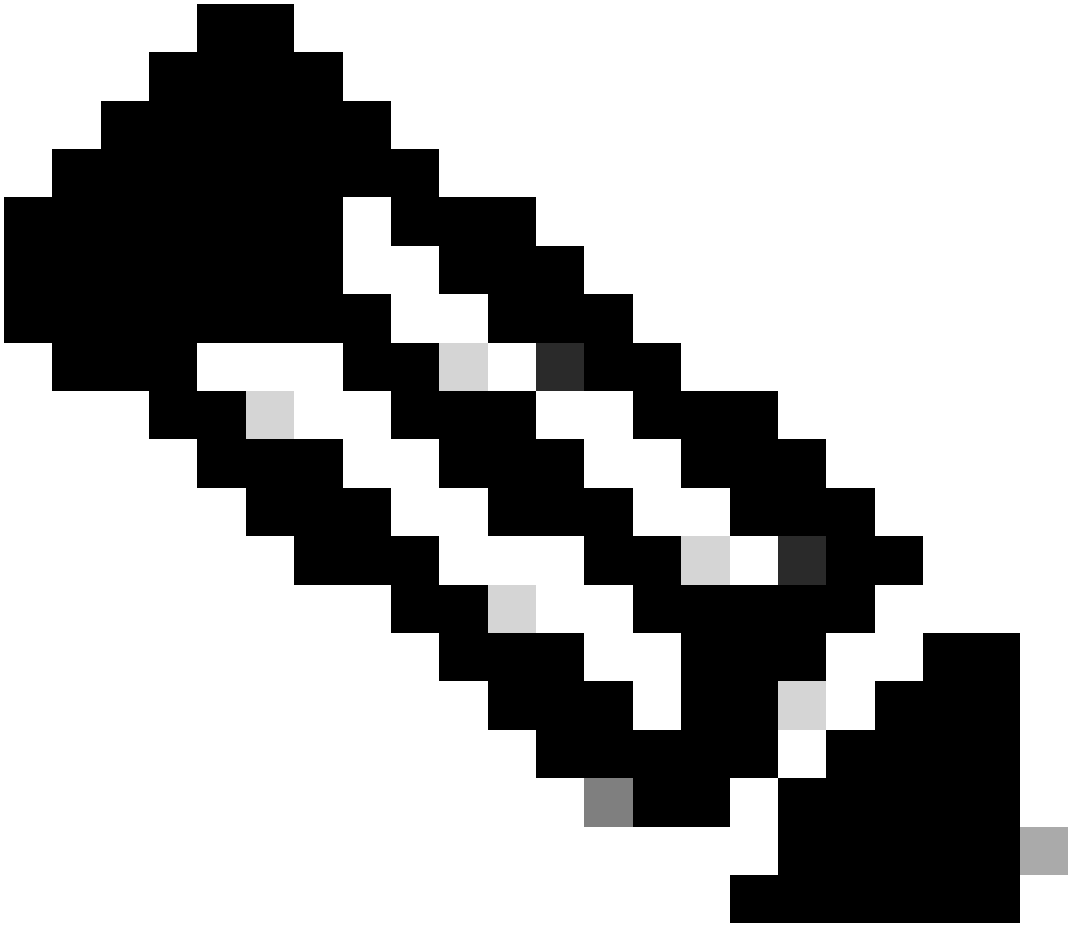
¿Qué es STIX/TAXI?

STIX (Expresión estructurada de información de amenazas)

STIX es un formato estandarizado que se utiliza para describir la inteligencia de amenazas cibernéticas (CTI), incluidos indicadores, tácticas, técnicas, malware y agentes de amenazas, de una manera estructurada y legible por máquina. Una fuente STIX normalmente incluye indicadores, patrones que ayudan a detectar actividades cibernéticas sospechosas o maliciosas.

TAXI (Intercambio automatizado de confianza de información de inteligencia)

TAXI es un protocolo utilizado para intercambiar datos STIX entre sistemas de forma segura y automática. Define cómo se intercambia la inteligencia de amenazas cibernéticas entre sistemas, productos u organizaciones mediante servicios dedicados (servidores TAXI).



Nota: La versión AsyncOS 16.0 admite las versiones STIX/TAXI: STIX 1.1.1 y 1.2, con TAXI 1.1.

Fuentes de fuente

Los dispositivos de seguridad de correo electrónico pueden consumir fuentes de inteligencia de amenazas de diversas fuentes, incluidos repositorios públicos, proveedores comerciales y sus propios servidores privados dentro de la organización.

Para garantizar la compatibilidad, todas las fuentes deben utilizar las normas STIX/TAXI, que permiten el intercambio estructurado y automatizado de datos sobre amenazas.

Biblioteca en cabina

La biblioteca Cabby Python es una herramienta útil para conectarse a servidores TAXI, descubrir colecciones STIX y sondear datos de amenazas. Es una excelente manera de probar y validar que una fuente de alimentación funciona correctamente y devuelve los datos según lo esperado antes de integrarlos en su dispositivo de seguridad de correo electrónico.

Instalación de Cabby Library

Para instalar la biblioteca Cabby, debe asegurarse de que su máquina local tenga instalado Python pip.

Una vez instalado python pip, solo necesita ejecutar este comando para instalar la biblioteca cabby.

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

Una vez finalizada la instalación de la biblioteca de taxii, puede verificar que los comandos taxii-collection y taxii-poll estén 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] [--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 - Pulsos y fuentes

Para empezar a descubrir información de AlienVault, cree primero una cuenta en el sitio de AlienVault y, a continuación, comience a buscar la información que desee.

En AlienVault, las fuentes y los pulsos están relacionados pero no son los mismos:

Impulsos

Los pulsos se seleccionan con inteligencia de amenazas con indicadores agrupados + contexto (legible por las personas).

- Un pulso es un conjunto de indicadores de amenazas (IOC) agrupados en torno a una amenaza o campaña específica.
- Creado por la comunidad o los proveedores para describir cosas como malware, phishing o ransomware.
- Cada pulso incluye contexto como descripción de amenazas, indicadores asociados (IP, dominio, hash de archivo, etc.), etiquetas y referencias.
- Los pulsos son legibles por el ser humano y están estructurados de una manera que se puede entender y compartir fácilmente.

Piense en un pulso como en un informe de amenazas con IOC y metadatos agrupados.

Fuentes

Las fuentes son un flujo automatizado de indicadores de varios pulsos (legibles por máquina).

- Las fuentes son un flujo de indicadores sin procesar (IOC) extraídos de uno o más pulsos, normalmente de forma automatizada.
- Normalmente, las herramientas de seguridad las utilizan para ingerir indicadores de forma masiva, a través de formatos como STIX/TAXI, CSV o JSON.
- Las fuentes se centran en las máquinas y se utilizan para la automatización y la integración con SIEM, firewalls y gateways de correo electrónico.

Una fuente tiene más que ver con el mecanismo de distribución, mientras que un pulso es el contenido y el contexto de la amenaza.

Normalmente se sondean las fuentes y éstas se componen de indicadores extraídos de los pulsos.

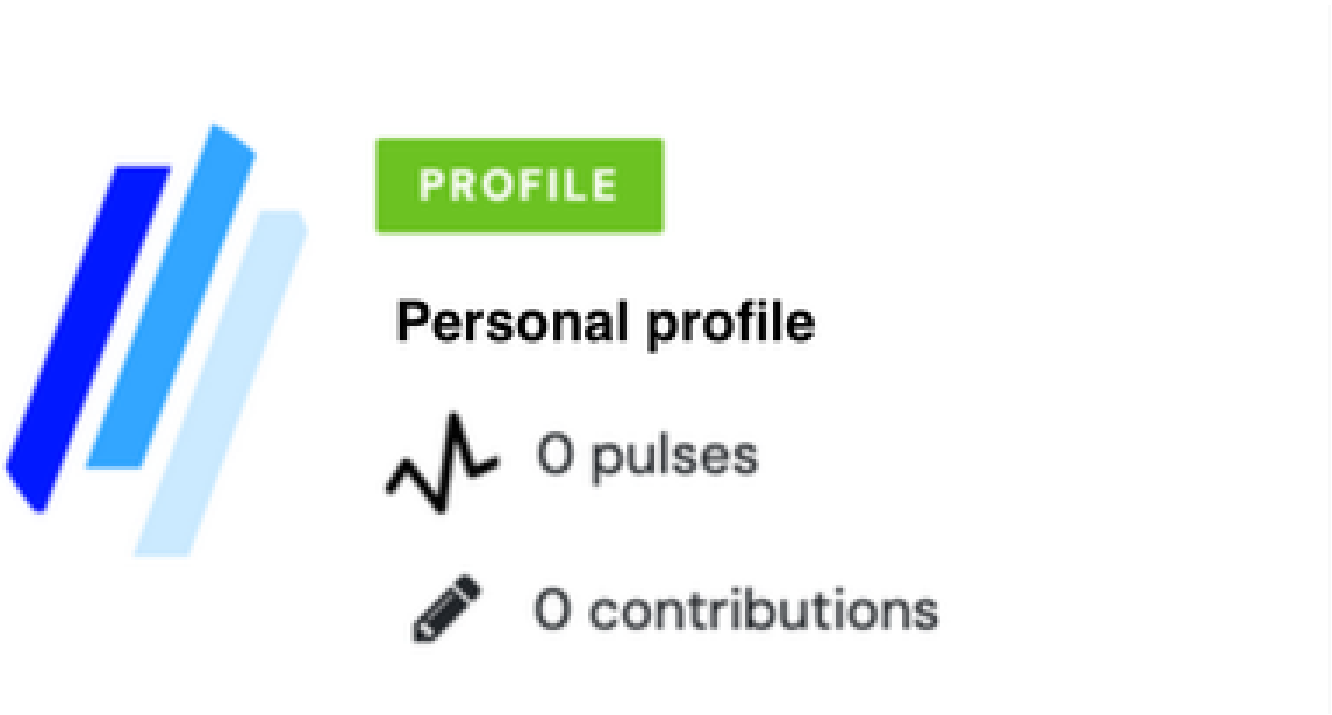
Iniciar recopilación de sondeo

Sondeo desde su propio perfil

Una vez que tenga su cuenta de AlienVault, puede comenzar a utilizar los comandos taxii-collection y taxii-poll.

Así es como se utilizan estos comandos para este caso de uso:

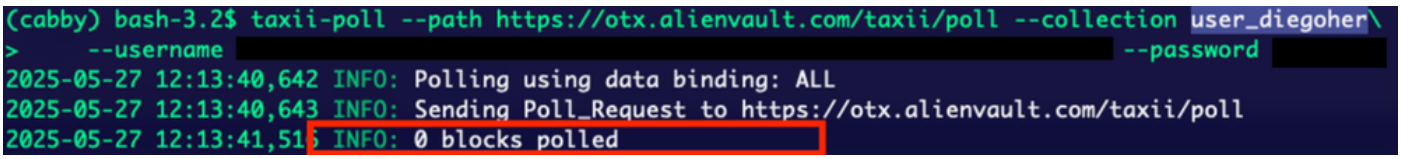
En este caso, dentro del perfil de AlienVault, no hay pulsos disponibles, pero como prueba, puede sondear una colección de su perfil usando el comando taxii-poll:



perfil personal de alienvault

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

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

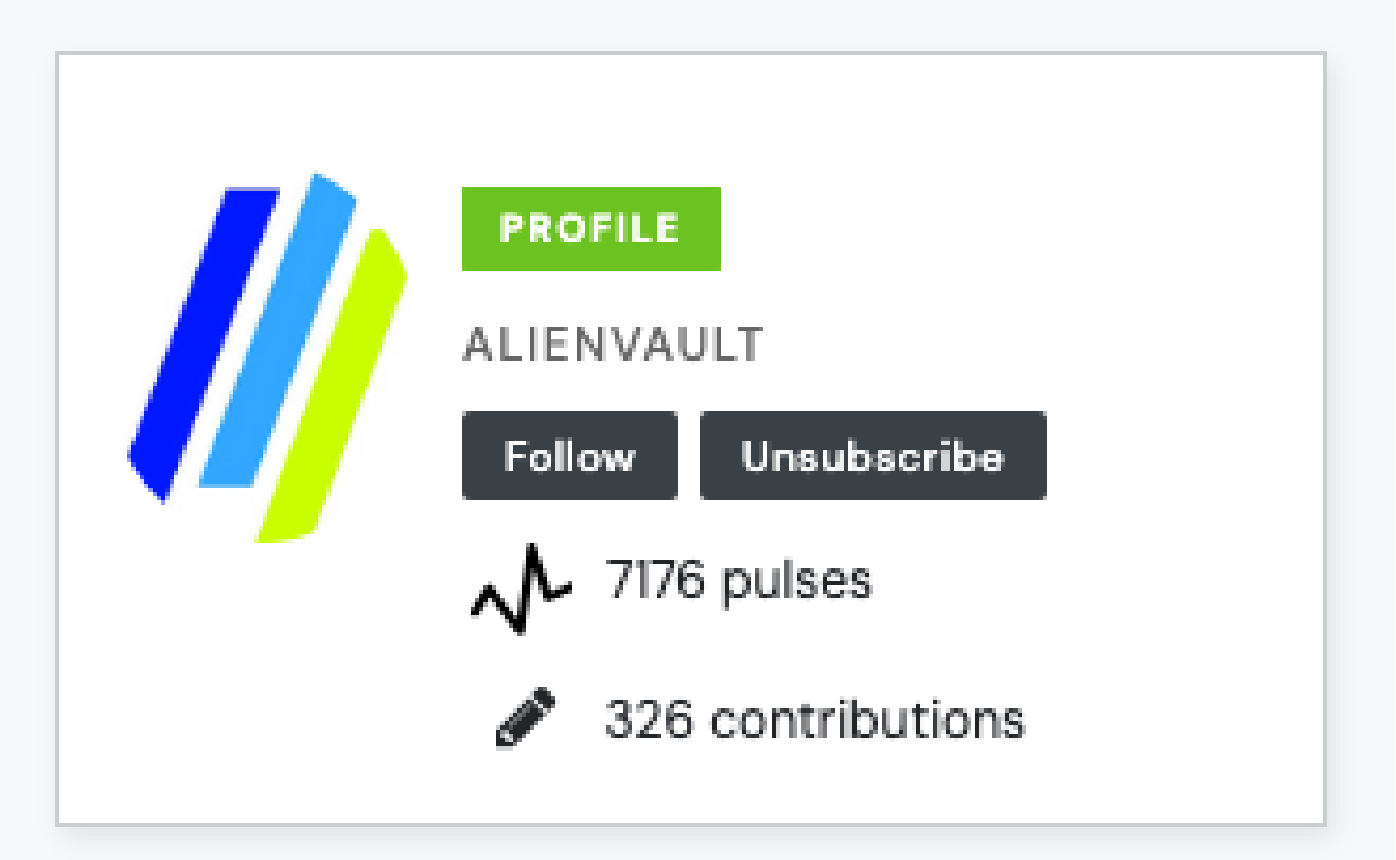


perfil personal de sondeo

Como puede ver, no hay bloques sondeados porque no hay información disponible en el perfil de AlienVault.

Sondeo desde perfiles de AlienVault

Una vez que se descubren los perfiles dentro de AlienVault, algunos de ellos tienen pulsos. En este ejemplo, se utiliza el perfil AlienVault.



perfil alienvault

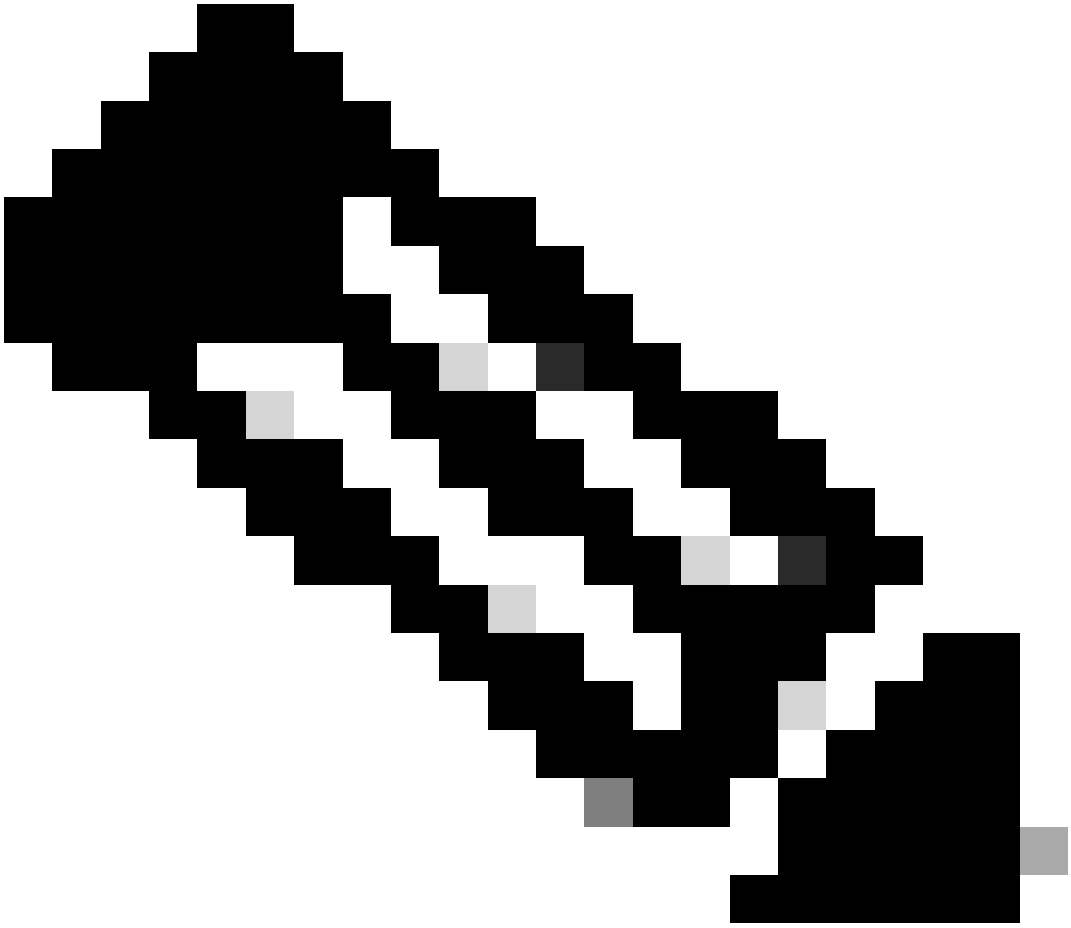
Cuando se ejecuta la encuesta con el comando taxii-poll, inmediatamente comienza a obtener toda la información del perfil.

```
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

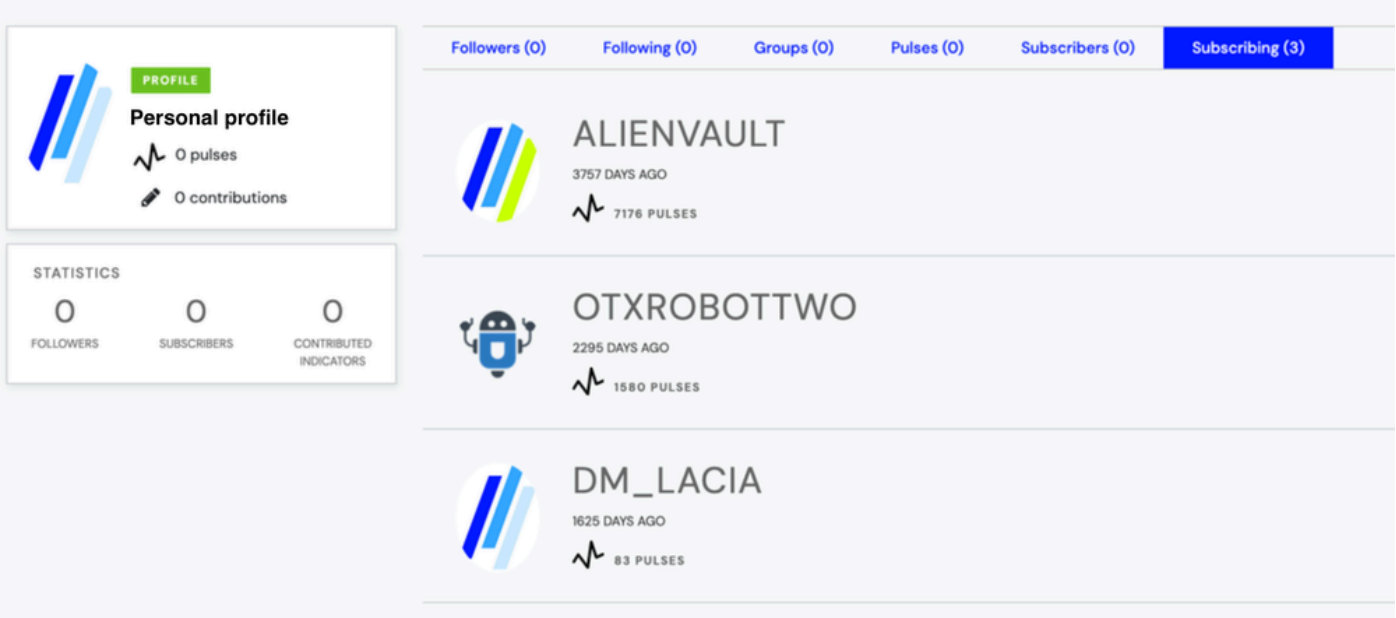
Como se muestra, el proceso comienza a obtener la información.



Nota: Para saber cuál es su nombre de usuario y contraseña, consulte este enlace https://otx.alienvault.com/api

Suscripciones a la colección de perfiles AlienVault

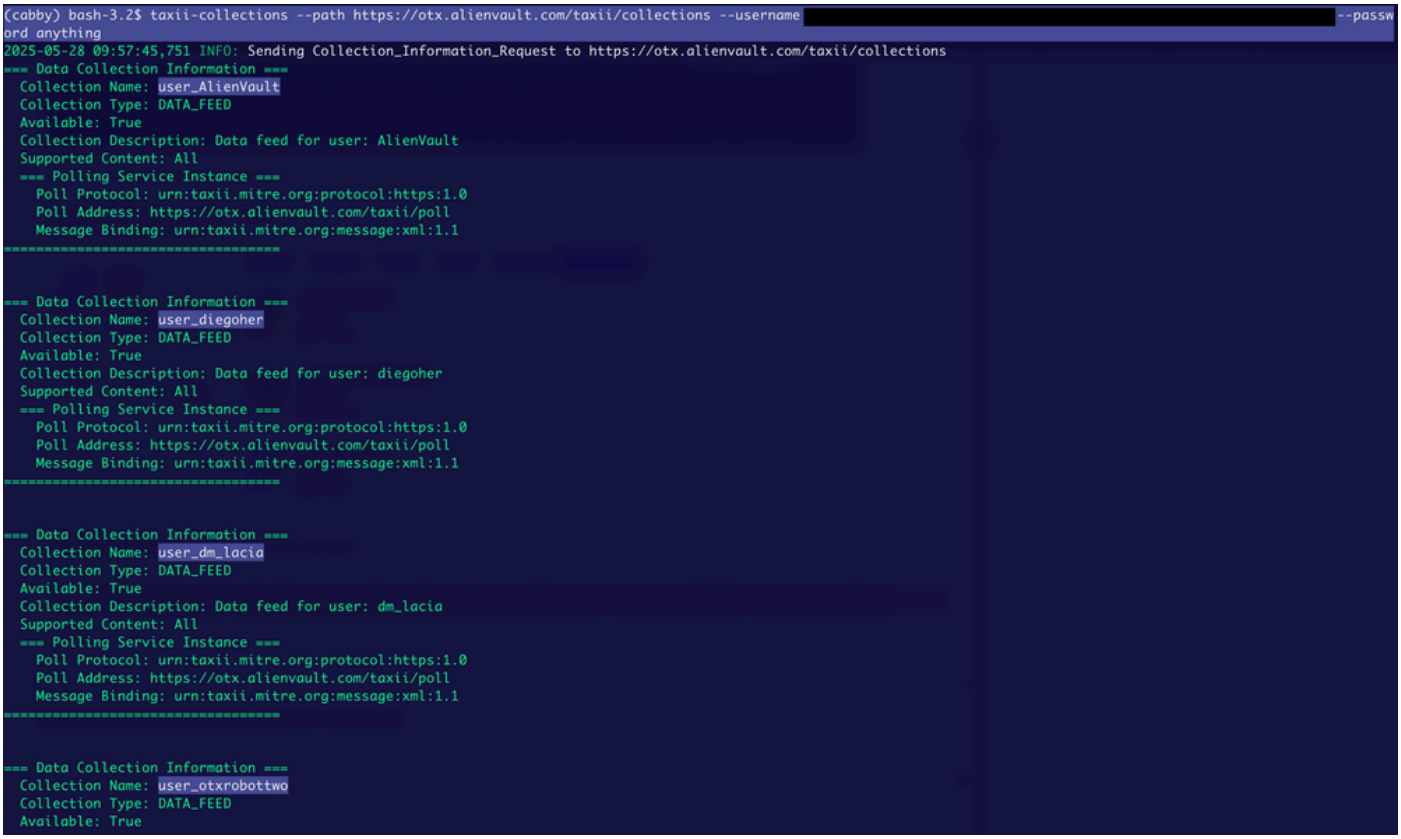
Como prueba, este usuario se suscribió a 3 perfiles.



suscripciones del perfil personal

Puede utilizar el comando taxii-collection para obtener esas suscripciones.

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



colecciones de perfiles personales

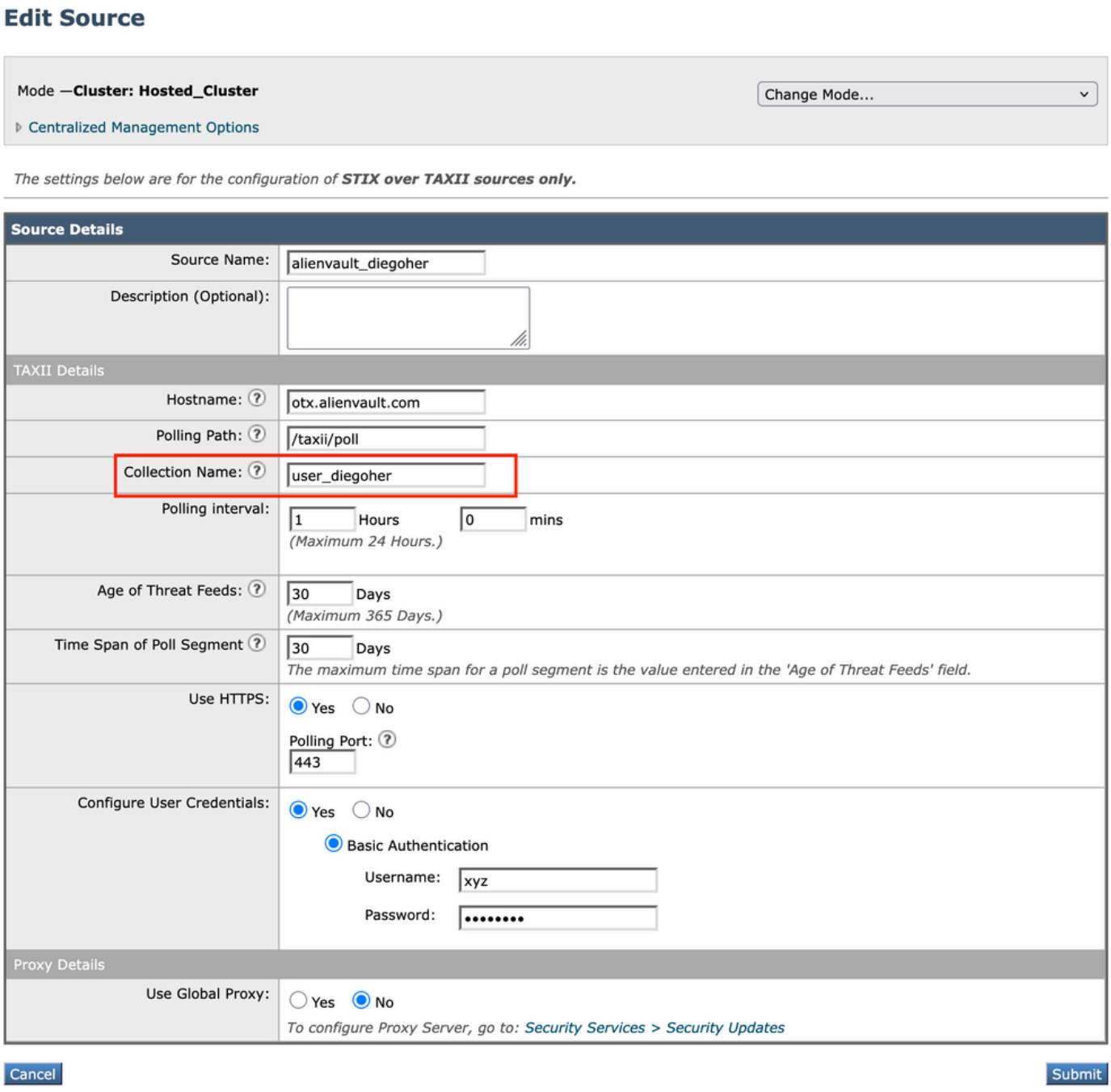
Puede confirmar que el comando taxii-collection funciona si el nombre de la colección es el mismo

que el de la suscripción.

Adición de orígenes a ESA

Agregar origen sin fuentes

1. Vaya a Políticas de correo > Administrador de fuentes de amenazas externas.
2. Cambie al modo de clúster.
3. Haga clic en Agregar origen.
4. Hostname: otx.alienvault.com
5. Ruta de sondeo: /taxi/poll
6. Nombre de la colección: user_<your_AlienVault_username>
7. Puerto: 443
8. Configurar credenciales de usuario: El que AlienVault le proporcionó.
9. Haga clic en Submit > Commit Changes.



fuente personal

Fuente de sondeo sin fuentes

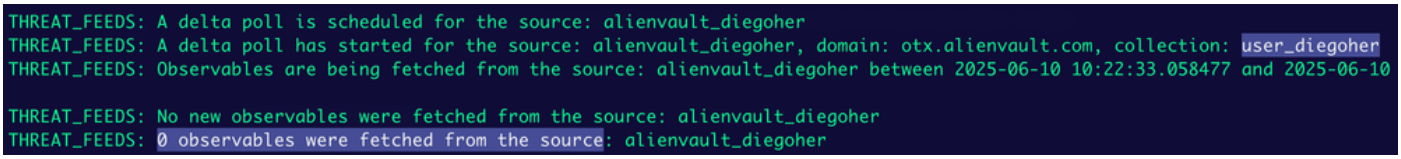
En el Administrador de fuentes de amenazas externas, después de agregar el origen, el origen recién agregado se hace visible.

información personal

Una vez agregado, haga clic en Sondear ahora.

Verificación

Inicie sesión en el ESA mediante CLI y revise los registros de la fuente de amenazas para verificar la información.

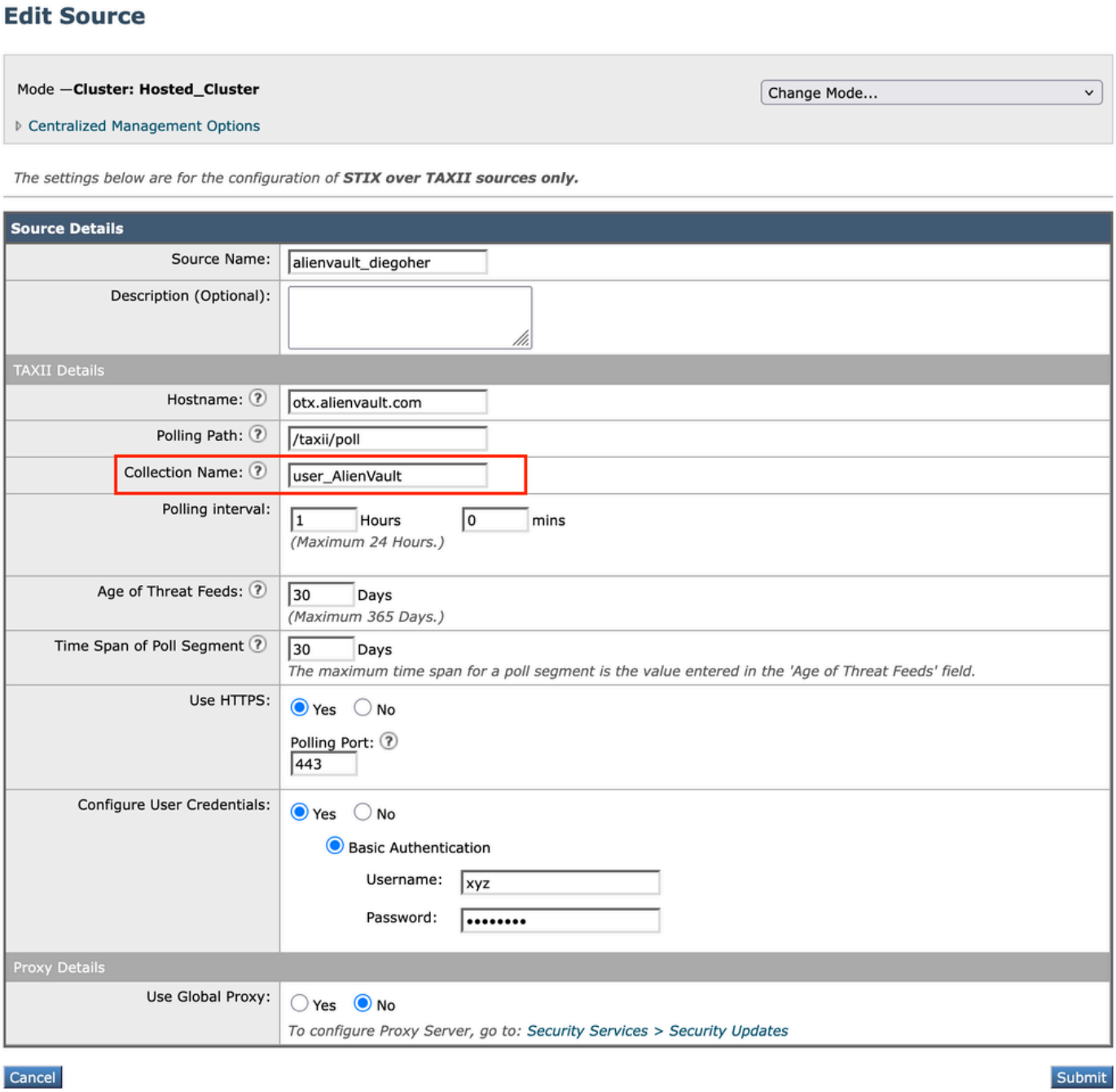


Encuesta personal ETF

Como se muestra en la imagen, puede ver que se obtuvieron 0 observables y esto se espera porque no hay fuentes en el perfil que se muestra.

Agregar origen con fuentes

1. Vaya a Políticas de correo > Administrador de fuentes de amenazas externas.
2. Cambie al modo de clúster.
3. Haga clic en Agregar origen.
4. Hostname: otx.alienvault.com
5. Ruta de sondeo: /taxi/poll
6. Nombre de la colección: user_AlienVault
7. Puerto: 443
8. Configurar credenciales de usuario: El que AlienVault le proporcionó.
9. Haga clic en Submit > Commit Changes.



alienvault source

Fuente de sondeo con fuentes

En el Administrador de fuentes de amenazas externas, después de agregar el origen, el origen recién agregado se hace visible.

fuente alienvault

Una vez agregado, haga clic en Sondear ahora.

Verificación

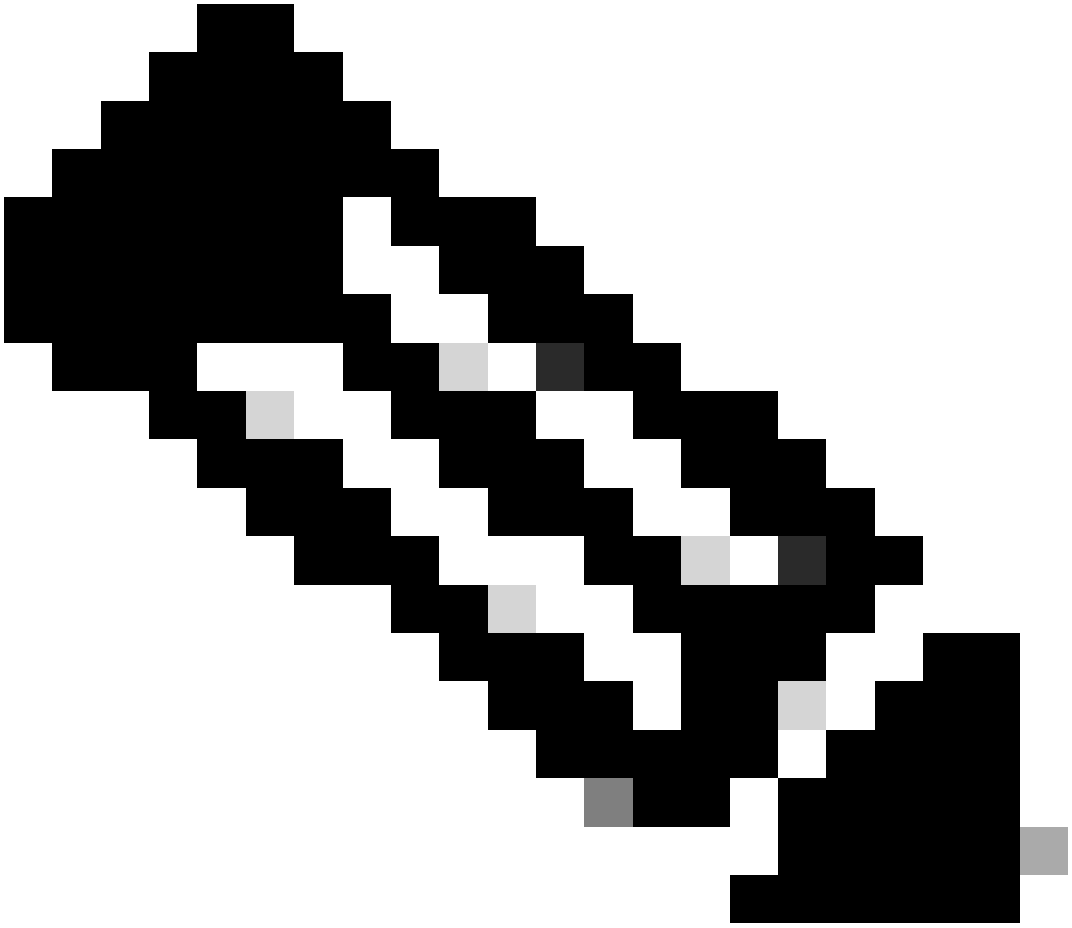
Inicie sesión en el ESA mediante CLI y revise los registros de la fuente de amenazas para verificar la información.

```
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
```

fuente de sondeo alienvault

Como se muestra en la imagen, se puede ver que se obtuvieron varios observables.



Nota: Si se agregan nuevas fuentes a la colección configurada, el ESA sondea automáticamente el origen y se obtienen los nuevos observables.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).