Configurar o AlienVault como um feed de ameaças externo para o ESA

Contents

Introdução

Este documento descreve as etapas para configurar feeds de ameaças externas de uma fonte AlienVault e usá-los no ESA.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Cisco Secure Email Gateway (SEG / ESA) AsyncOS 16.0.2
- CLI do Linux
- Pip Python3
- Conta do AlienVault

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivo de segurança de e-mail
- Python3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A estrutura de Feeds Externos de Ameaças (ETF) permite que o gateway de e-mail inclua inteligência de ameaças externas compartilhada no formato STIX por meio do protocolo TAXII. Ao aproveitar esse recurso, as organizações podem:

- Adote uma postura proativa contra ameaças cibernéticas, como malware, ransomware, phishing e ataques direcionados.
- Inscreva-se em fontes de inteligência de ameaças locais e de terceiros.
- Aumente a eficácia geral do gateway de e-mail.

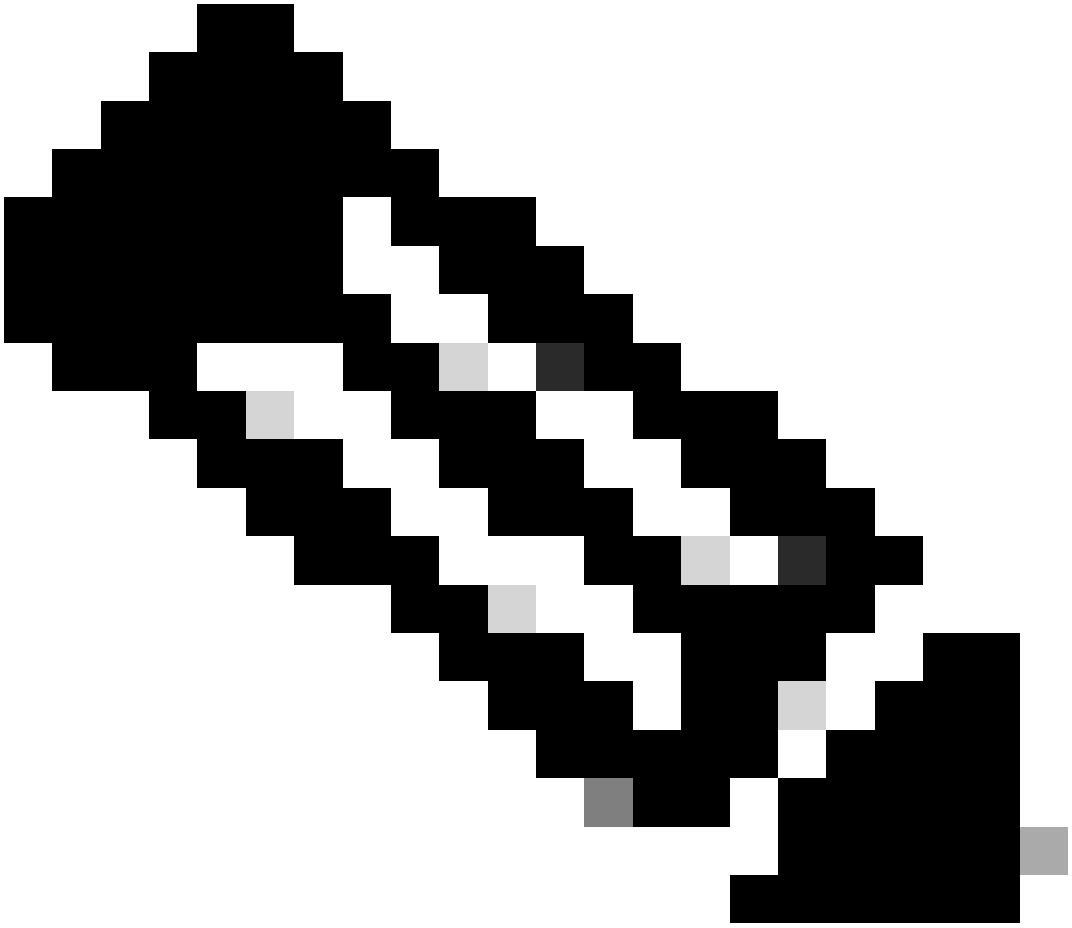
O que é o STIXX/TAXII?

STIX (Expressão de Informações de Ameaças Estruturadas)

STIX é um formato padronizado usado para descrever a inteligência de ameaças cibernéticas (CTI), incluindo indicadores, táticas, técnicas, malware e agentes de ameaças, de forma estruturada e legível por máquina. Um feed STIX normalmente inclui indicadores, padrões que ajudam a detectar atividades cibernéticas suspeitas ou mal-intencionadas.

TAXII (Trusted Automated Exchange of Intelligence Information, Intercâmbio automatizado confiável de informações de inteligência)

O TAXII é um protocolo usado para trocar dados STIX entre sistemas de forma segura e automática. Define como a inteligência de ameaças cibernéticas é trocada entre sistemas, produtos ou empresas por meio de serviços dedicados (servidores TAXII).



Observação: a versão 16.0 do AsyncOS suporta as versões STIX/TAXII: STIX 1.1.1 e 1.2, com TAXII 1.1.

Fontes de alimentação

Os dispositivos de segurança de e-mail podem consumir feeds de inteligência de ameaças de várias fontes, incluindo repositórios públicos, provedores comerciais e seus próprios servidores privados na empresa.

Para garantir a compatibilidade, todas as fontes devem usar os padrões STIX/TAXII, que permitem o compartilhamento estruturado e automatizado de dados de ameaças.

Biblioteca Cabby

A biblioteca Cabby Python é uma ferramenta útil para se conectar a servidores TAXII, descobrindo coleções STIX e fazendo polling de dados de ameaças. É uma ótima maneira de testar e validar se uma fonte de alimentação está funcionando corretamente e retornando os dados como esperado antes de integrá-los ao seu dispositivo de segurança de e-mail.

Instalando a Biblioteca Cabby

Para instalar a biblioteca Cabby, você precisa certificar-se de que sua máquina local tenha o Python pip instalado.

Uma vez que o python pip estiver instalado, você só precisa executar este comando para instalar a biblioteca cabby.

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

Quando a instalação da biblioteca de cabeamento estiver concluída, você poderá verificar se os comandos taxii-collection e taxii-poll estão disponíveis agora.

```
(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 e Feeds

Para começar a descobrir informações do AlienVault, primeiro crie uma conta no site do AlienVault e, em seguida, comece a procurar as informações desejadas.

No AlienVault, os feeds e pulsos estão relacionados, mas não são os mesmos:

Pulsos

Os pulsos são uma ameaça com curadoria da intel com indicadores agrupados + contexto (legível por humanos).

- Um pulso é uma coleção de indicadores de ameaças (IOCs) agrupados em torno de uma ameaça ou campanha específica.
- Criado pela comunidade ou por provedores para descrever coisas como malware, phishing e ransomware.
- Cada pulso inclui contexto, como descrição da ameaça, indicadores associados (IP, domínio, hash de arquivo e assim por diante), marcas e referências.
- Os pulsos são legíveis por humanos e estruturados de uma forma que pode ser facilmente compreendida e compartilhada.

Pense em um pulso como um relatório de ameaças com IOCs e metadados agrupados.

Feeds

Feeds são fluxos automatizados de indicadores de vários pulsos (legíveis por máquina).

- Feeds são um fluxo de indicadores brutos (IOCs) extraídos de um ou mais pulsos, geralmente de forma automatizada.
- Eles são geralmente usados por ferramentas de segurança para incluir indicadores em massa, através de formatos como STIX/TAXII, CSV ou JSON.
- Os feeds são focados na máquina e usados para automação e integração com SIEMs, firewalls e gateways de e-mail.

Um feed é mais sobre o mecanismo de entrega, enquanto um pulso é o conteúdo e o contexto da ameaça.

Você normalmente pesquisa feeds, e esses feeds são compostos de indicadores extraídos de pulsos.

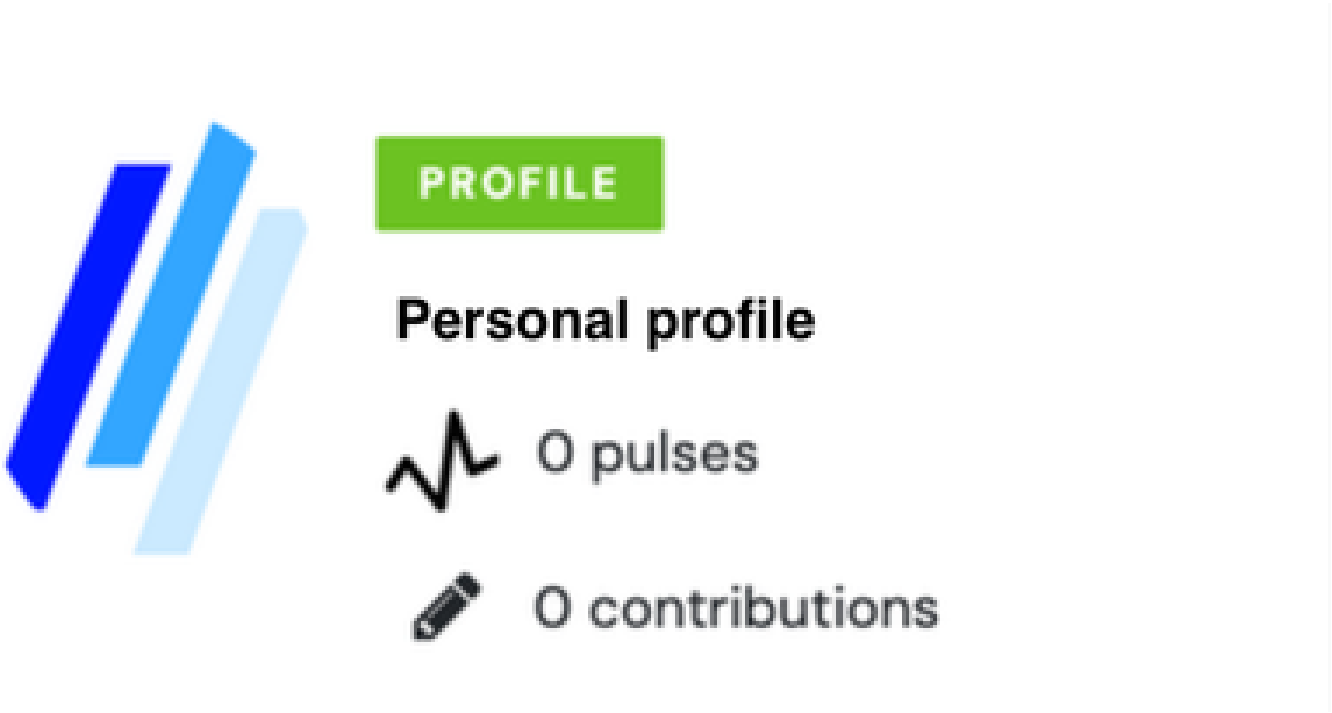
Iniciar Coleções de Sondagem

Sondagem no seu próprio perfil

Depois de ter sua conta do AlienVault, você pode começar a usar os comandos taxii-collection e taxii-poll.

Veja a seguir como usar esses comandos para este caso de uso:

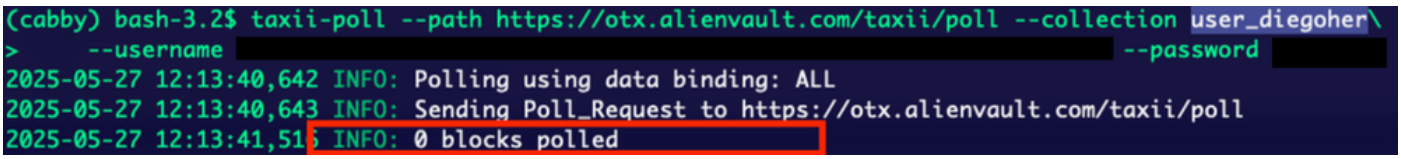
Nesse caso, no perfil do AlienVault, não há pulsos disponíveis, mas, como teste, você pode pesquisar uma coleção do seu perfil usando o comando taxii-poll:



perfil pessoal do alienvault

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

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

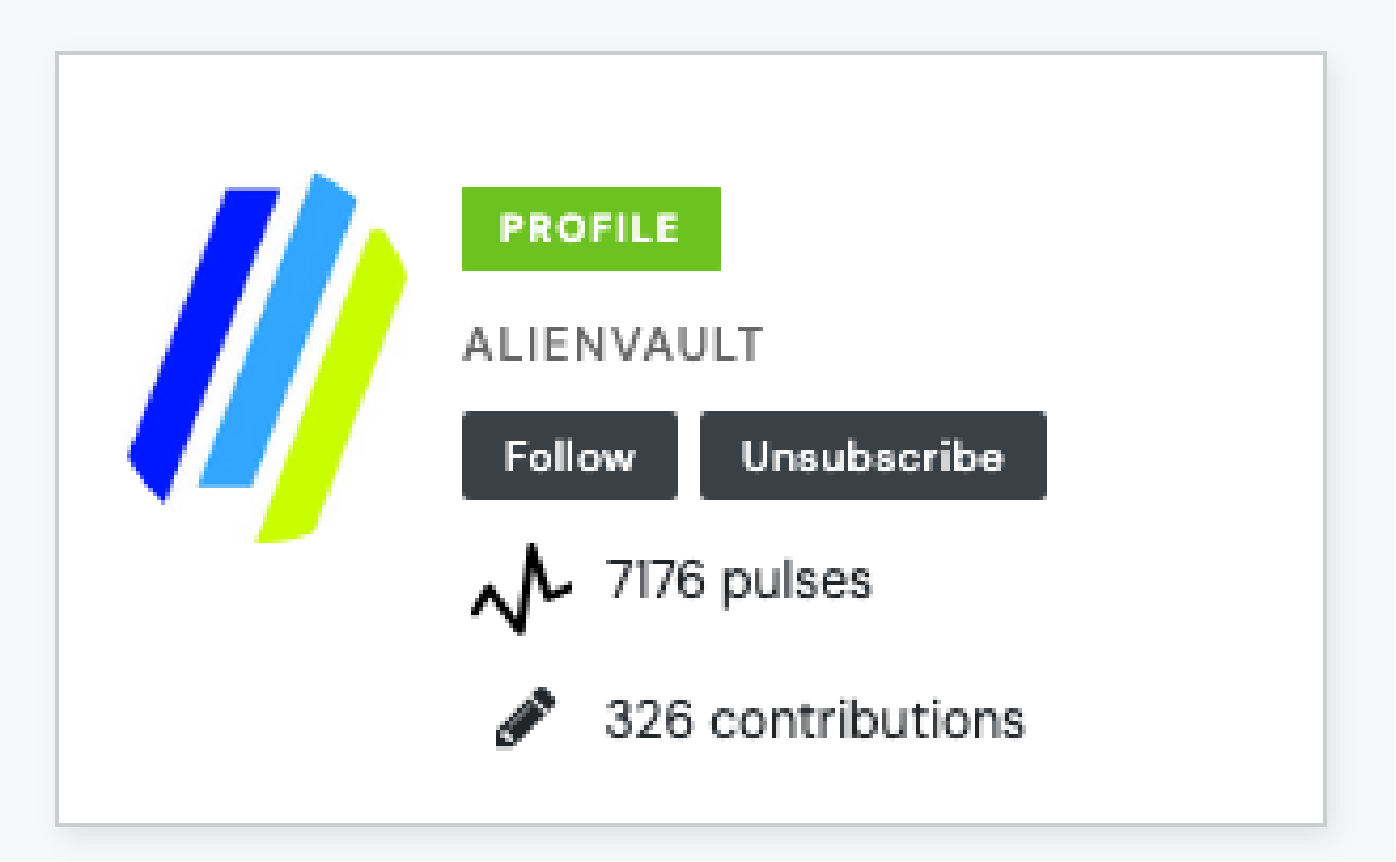


perfil pessoal da votação

Como você pode ver, não há blocos pesquisados porque não há informações disponíveis no perfil do AlienVault.

Sondagem de perfis do AlienVault

Quando os perfis dentro do AlienVault são descobertos, alguns deles têm pulsos. Neste exemplo, o perfil do AlienVault é usado.



perfil alienvault

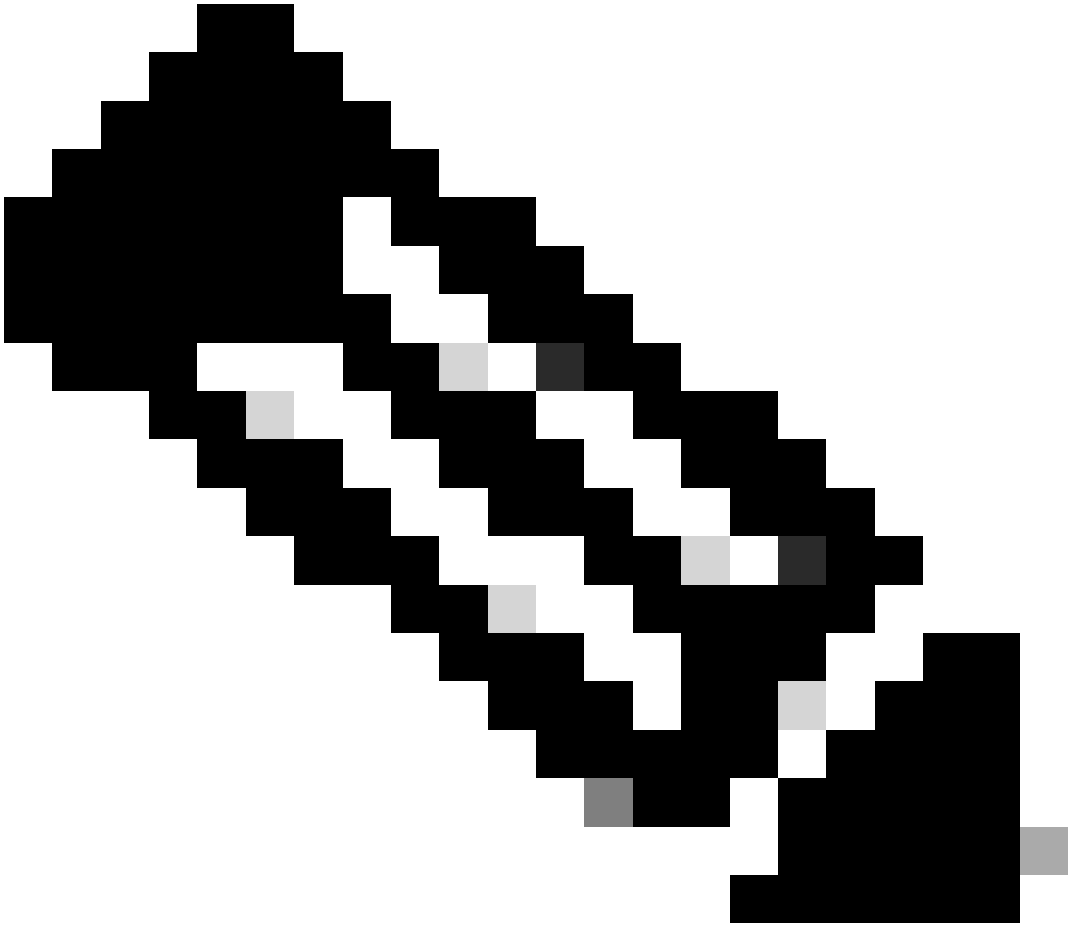
Ao executar a pesquisa com o comando taxii-poll, ele imediatamente inicia a busca de todas as informações do perfil.

```
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:/
```

pesquisa alienvault

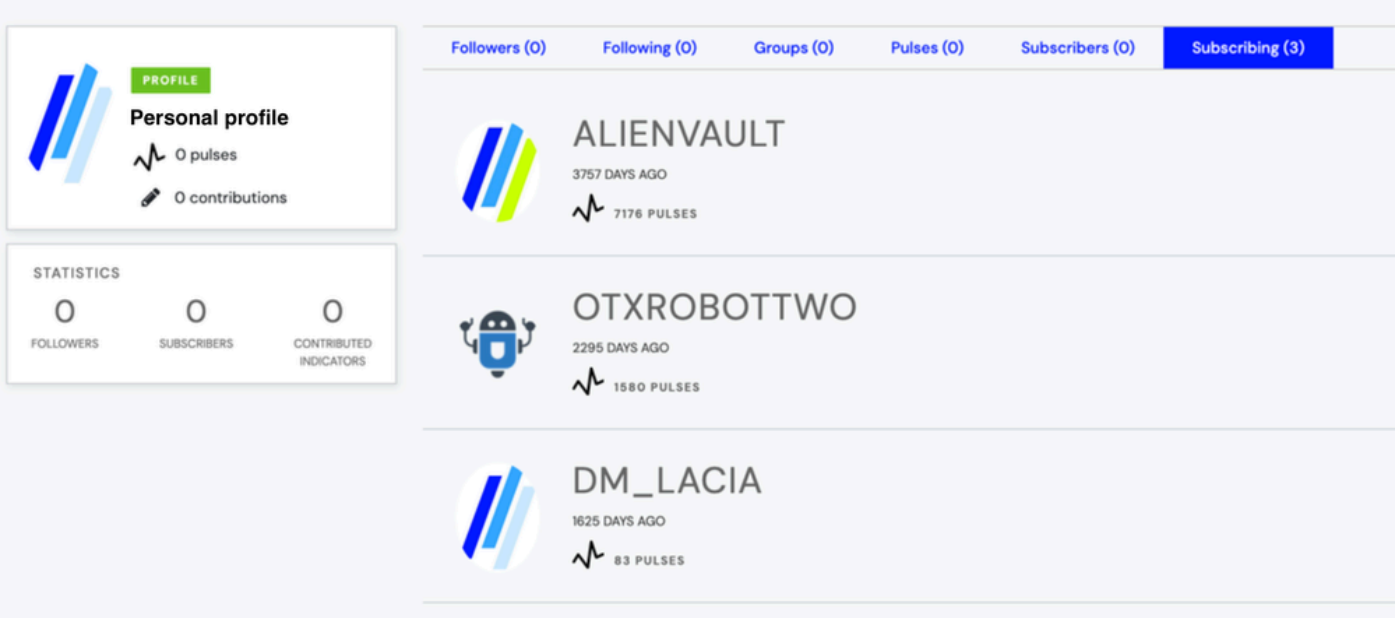
Como mostrado, o processo começa a buscar as informações.



Note: Para saber qual é o seu nome de usuário e senha, acesse este link https://otx.alienvault.com/api

Assinaturas da coleção de perfis do AlienVault

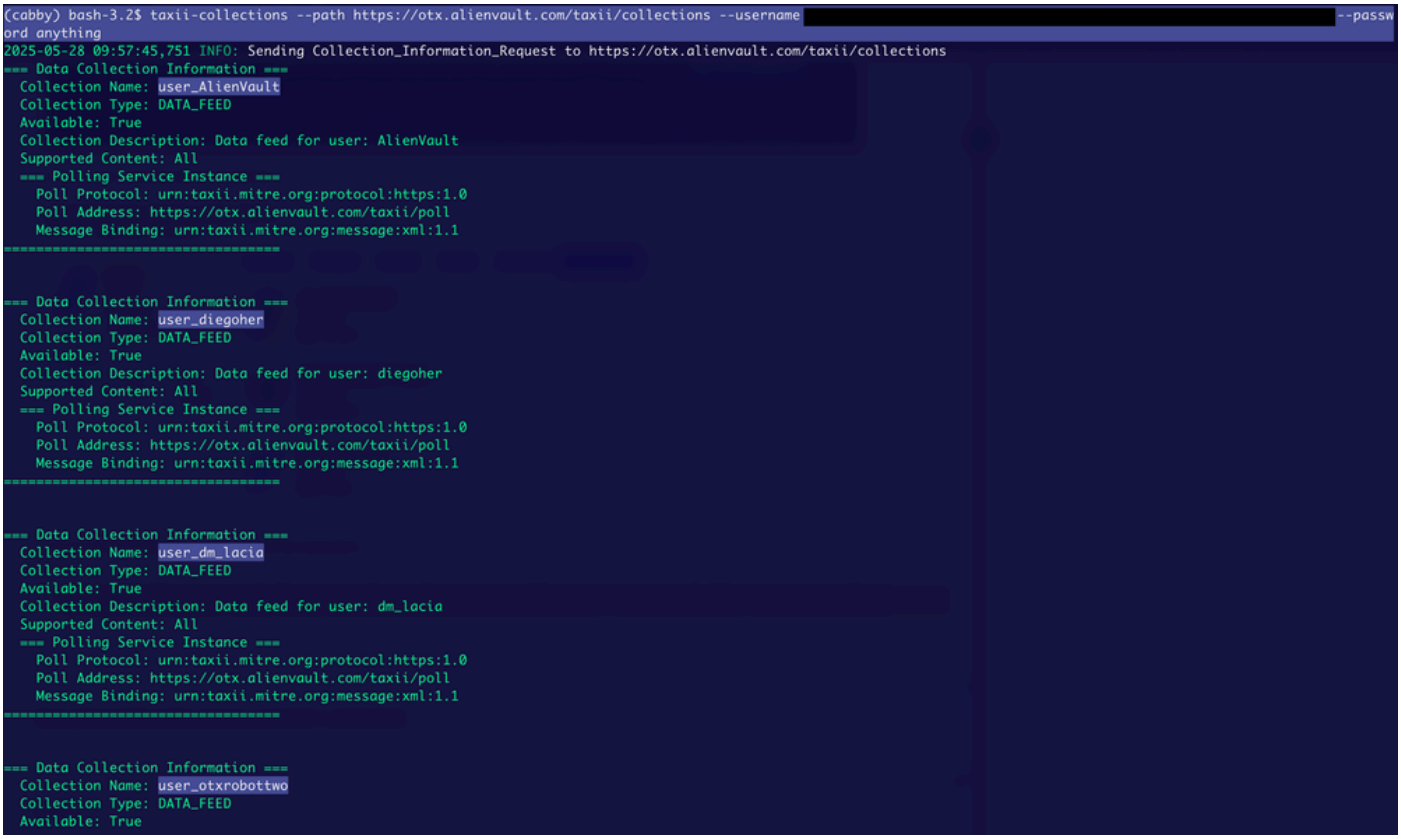
Como teste, este usuário assinou 3 perfis.



assinaturas de perfil pessoal

Você pode usar o comando taxii-collection para buscar essas assinaturas.

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



coleções de perfis pessoais

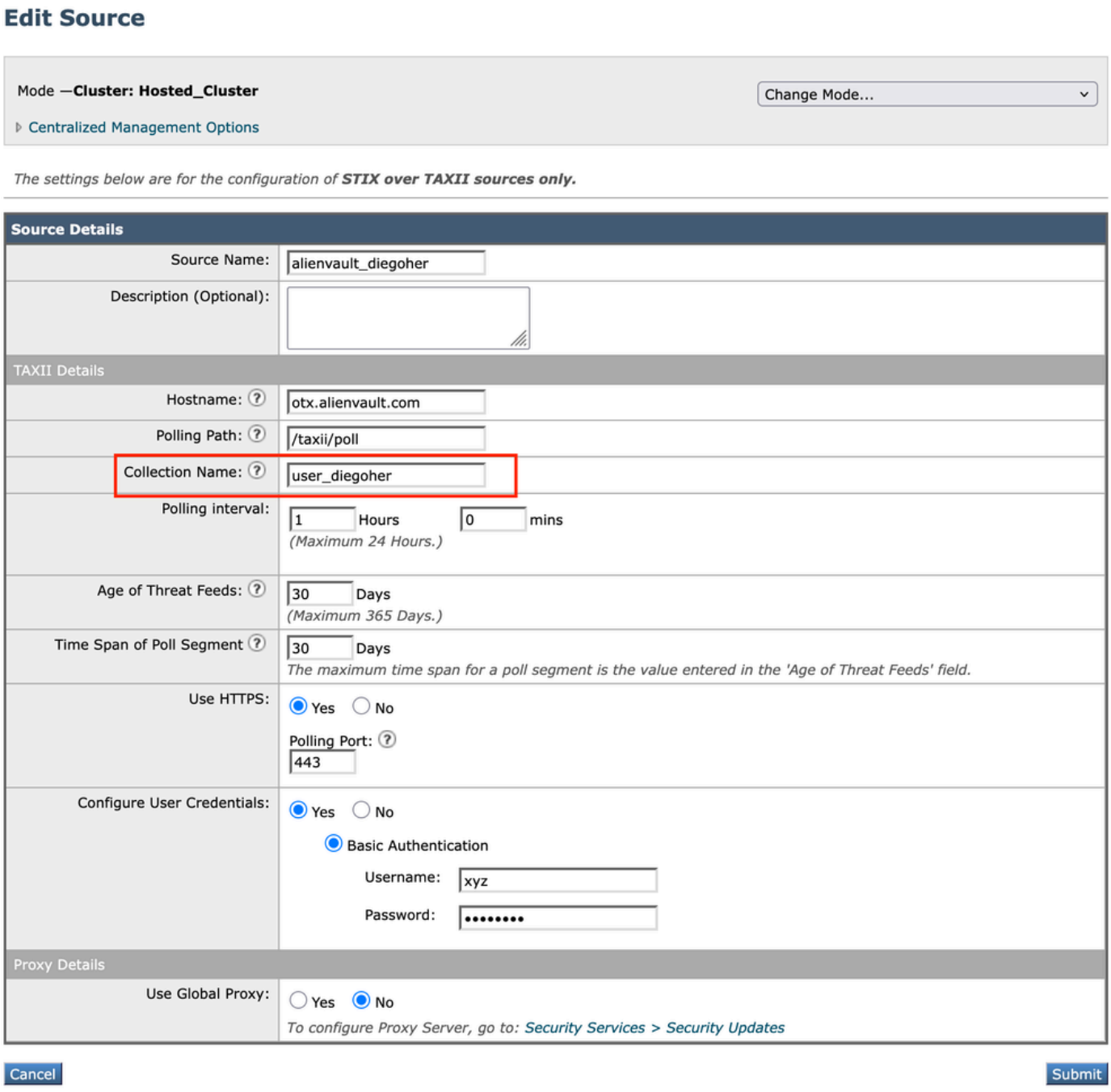
Você pode confirmar se o comando taxii-collection funciona se o Nome da coleção for o mesmo

que você assinou.

Adição de códigos-fonte ao ESA

Adicionando fonte sem feeds

1. Navegue até Políticas de e-mail > Gerenciador de feeds de ameaças externas.
2. Altere para Modo de cluster.
3. Clique em Add Source.
4. Hostname: otx.alienvault.com
5. Caminho de Sondagem: /taxi/poll
6. Nome da coleção: user_<your_AlienVault_username>
7. Porta: 443
8. Configurar credenciais do usuário: Aquele que o AlienVault forneceu a você.
9. Clique em Enviar > Confirmar alterações.



origem pessoal

Origem da Sondagem sem Feeds

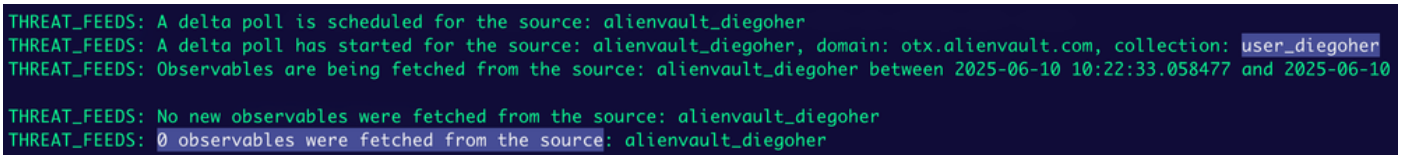
No Gerenciador de feeds de ameaças externas, depois que a origem é adicionada, a origem recém-adicionada torna-se visível.

feed pessoal

Depois de adicionada, clique em Votação Agora.

Verificar

Faça login no ESA via CLI e examine os registros de alimentação de ameaças para verificar as informações.

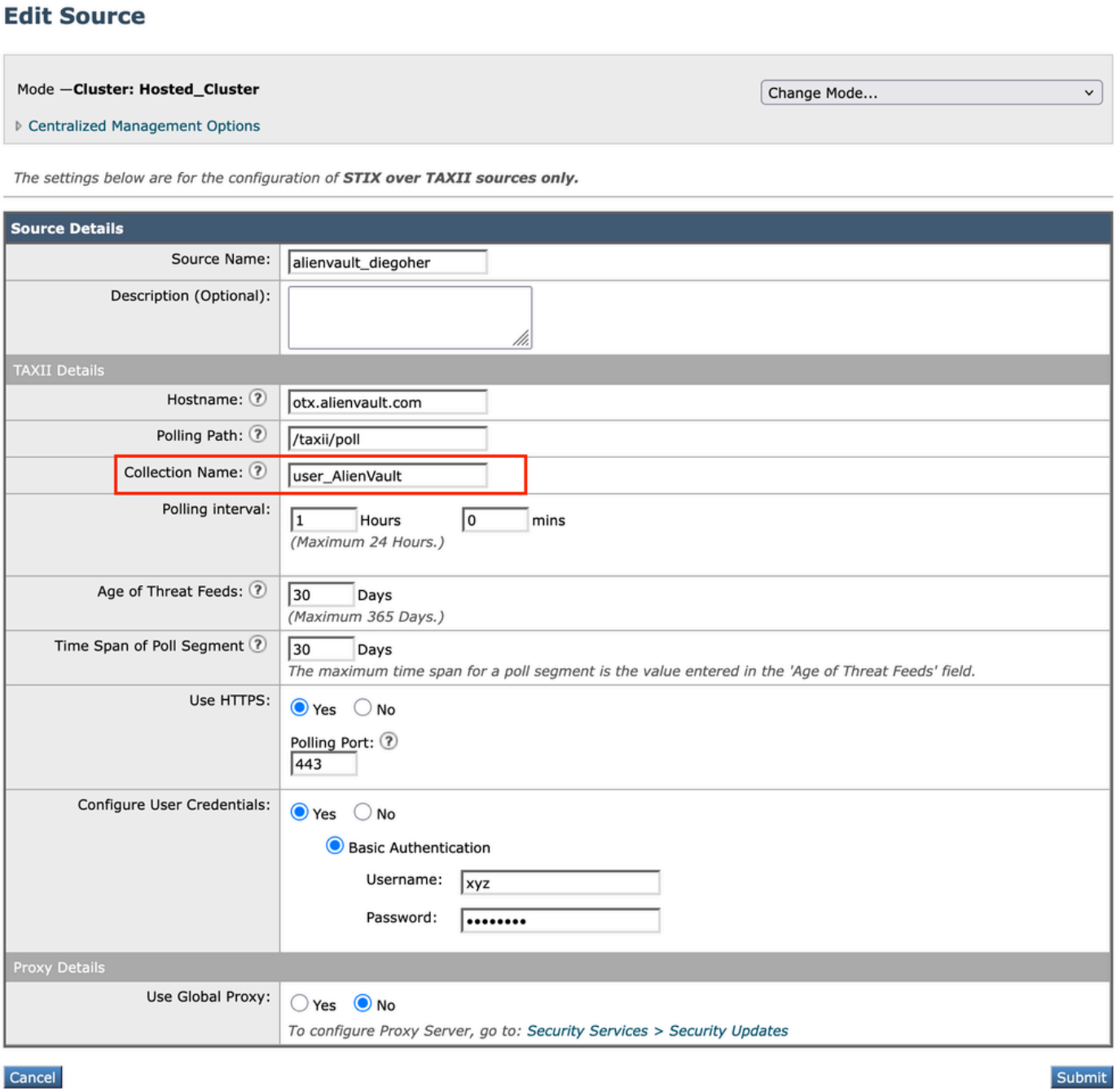


Pesquisa pessoal ETF

Como mostrado na imagem, você pode ver que 0 objetos de observação foram buscados e isso é esperado porque não há feeds no perfil mostrado.

Adicionando fonte com feeds

1. Navegue até Políticas de e-mail > Gerenciador de feeds de ameaças externas.
2. Altere para Modo de cluster.
3. Clique em Add Source.
4. Hostname: otx.alienvault.com
5. Caminho de Sondagem: /taxi/poll
6. Nome da coleção: user_AlienVault
7. Porta: 443
8. Configurar credenciais do usuário: Aquele que o AlienVault forneceu a você.
9. Clique em Enviar > Confirmar alterações.



origem de alienvault

Origem da Sondagem com Feeds

No Gerenciador de feeds de ameaças externas, depois que a origem é adicionada, a origem recém-adicionada torna-se visível.

feed alienvault

Depois de adicionada, clique em Votação Agora.

Verificar

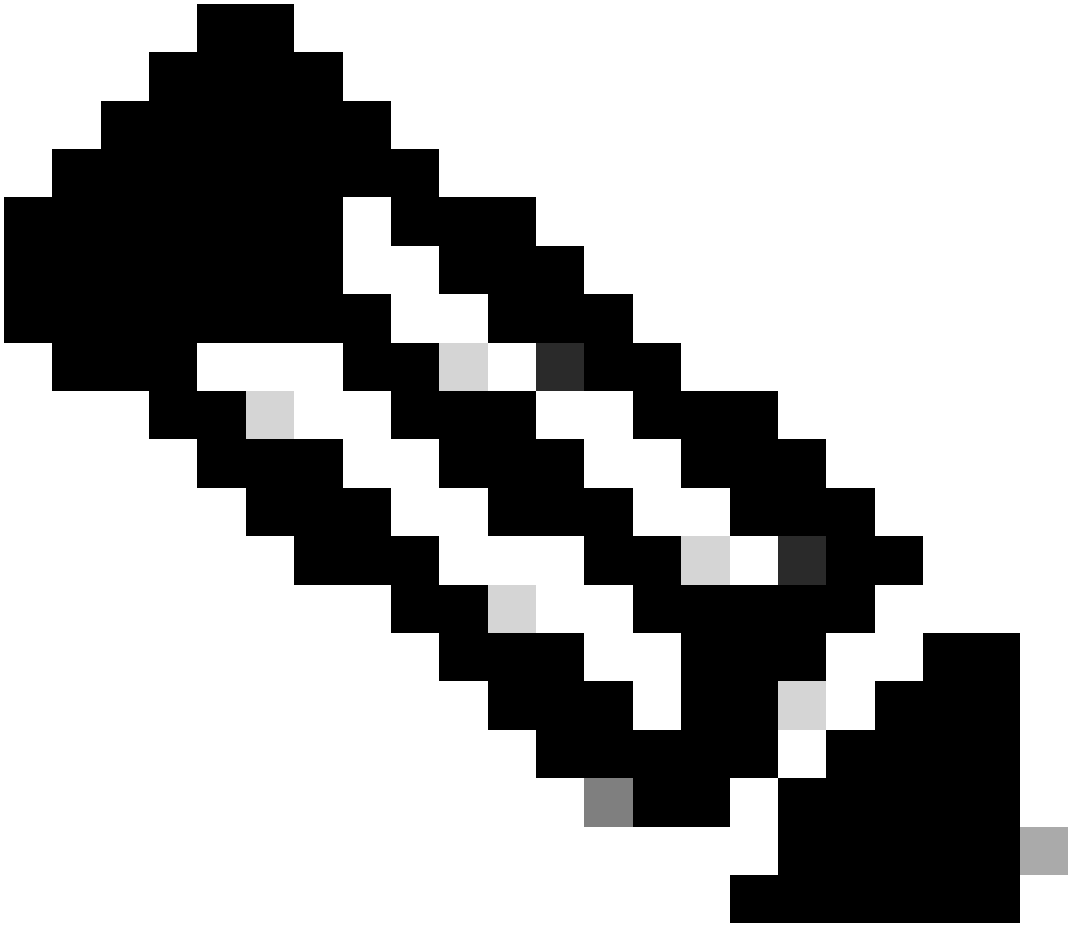
Faça login no ESA via CLI e examine os registros de alimentação de ameaças para verificar as informações.

```
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
```

sondando feed do alienvault

Como mostrado na imagem, você pode ver que vários observáveis foram buscados.



Note: Se novos feeds forem adicionados à coleção configurada, o ESA sondará automaticamente a origem e os novos observáveis serão buscados.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.