将AlienVault配置为ESA的外部威胁源

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

什么是STIX/TAXII?

- STIX（结构化威胁信息表达）
- TAXII（可信自动情报信息交换）

馈送源

Cabby库

- 安装Cabby库

AlienVault — 脉冲和源

- 脉冲
- 源

开始轮询收集

- 从自己的配置文件轮询
- 从AlienVault配置文件轮询
- AlienVault配置文件集合订阅

将源添加到ESA

- 添加没有源的源
- 无源的轮询源
- 验证
- 添加源与源
- 具有源的轮询源
- 验证

简介

本文档介绍从AlienVault源配置外部威胁源并在ESA中使用它的步骤。

先决条件

要求

建议掌握下列主题的相关知识：

- 思科安全电子邮件网关(SEG/ESA)AsyncOS 16.0.2
- Linux CLI

- Python3 pip
- AlienVault帐户

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 邮件安全设备
- Python3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

外部威胁源(ETF)框架使邮件网关能够通过TAXII协议接收以STIX格式共享的外部威胁情报。利用此功能，组织可以：

- 主动抵御网络威胁，例如恶意软件、勒索软件、网络钓鱼和有针对性的攻击。
- 订阅本地和第三方威胁情报源。
- 增强电邮网关的整体有效性。

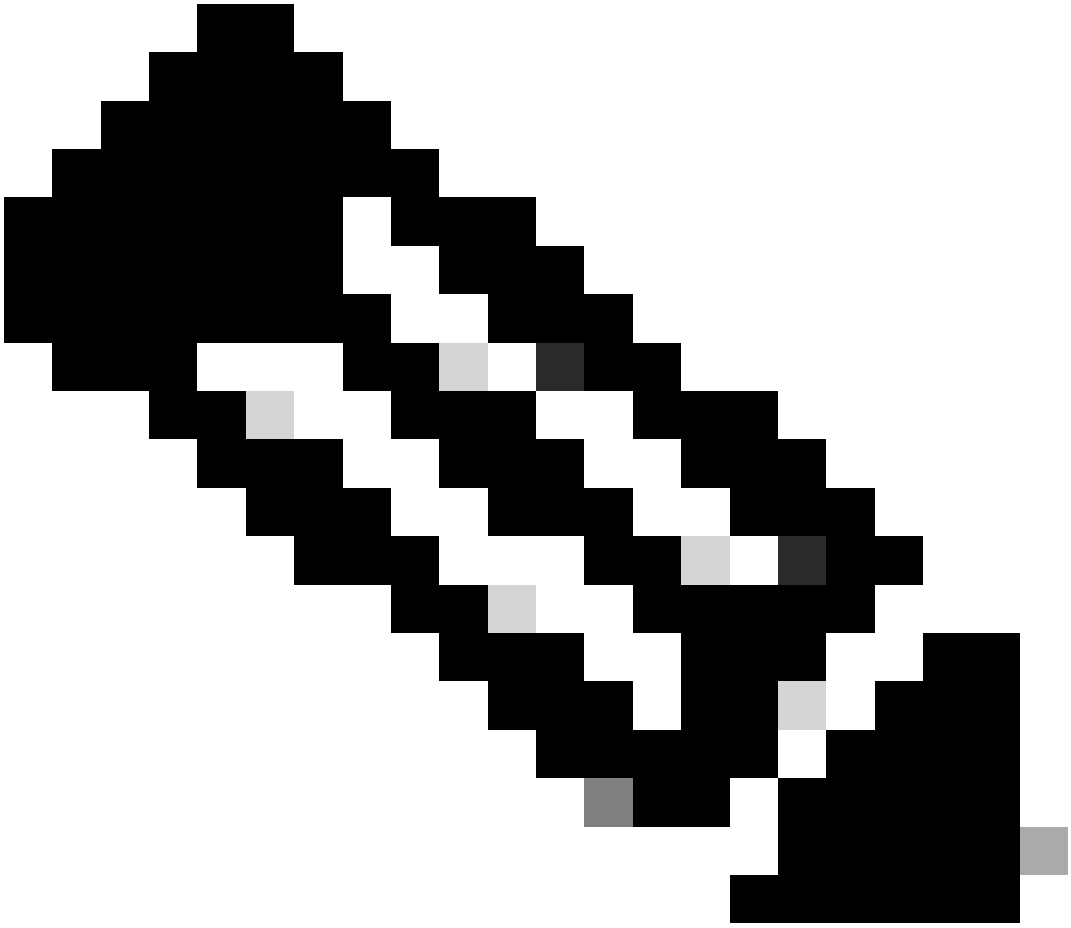
什么是STIX/TAXII?

STIX（结构化威胁信息表达）

STIX是一种标准化格式，用于以结构化和机器可读的方式描述网络威胁情报(CTI)，包括指标、战术、技术、恶意软件和威胁实施者。STIX馈送通常包含指示器 — 有助于检测可疑或恶意网络活动的模式。

TAXII（可信自动情报信息交换）

TAXII是一种用于在系统之间安全、自动地交换STIX数据的协议。定义如何在系统、产品或组织之间通过专用服务（TAXII服务器）交换网络威胁情报。



注意：AsyncOS 16.0版本支持STIX/TAXII版本：STIX 1.1.1和1.2,TAXII 1.1。

馈送源

邮件安全设备可以使用来自各种来源的威胁情报源，包括公共存储库、商业提供商以及您组织中的专用服务器。

为确保兼容性，所有来源都必须使用STIX/TAXII标准，该标准支持威胁数据的结构化自动共享。

Cabby库

Cabby Python库是连接到TAXII服务器、发现STIX集合和轮询威胁数据的有用工具。在将数据集成到邮件安全设备之前，这是一个很好的测试和验证源是否正常工作以及是否按预期返回数据的方式。

安装Cabby库

要安装Cabby库，您需要确保本地计算机已安装Python pip。

安装python pip后，只需运行此命令即可安装cabby库。

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

完成cabby库安装后，您可以验证taxii-collections和taxii-poll命令现在是否可用。

```
(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 — 脉冲和源

要开始发现AlienVault信息，请先在AlienVault站点上创建帐户，然后开始搜索所需信息。

在AlienVault中，源和脉冲是相关的，但不相同：

脉冲

脉冲是带有分组指示符+情景的威胁英特尔（人可读）。

- Pulse是围绕特定威胁或活动分组的威胁指标(IOC)的集合。
- 由社区或提供商创建，用于描述诸如恶意软件、网络钓鱼、勒索软件等内容。
- 每个脉冲包括威胁描述、相关指标（IP、域、文件哈希等）、标记和参考等情景。
- 脉冲是人类可读的，其结构方式易于理解和共享。

将脉冲视为具有分组IOC和元数据的威胁报告。

源

馈送是来自多个脉冲的指示器自动流（机器可读）。

- 源是从一个或多个脉冲提取的原始指示符(IOC)流，通常采用自动化方式。
- 安全工具通常使用它们通过STIX/TAXII、CSV或JSON等格式批量接收指标。
- 订阅源以机器为中心，用于自动化和与SIEM、防火墙和电邮网关集成。

馈送更多的是关于传送机制，而脉冲则是威胁的内容和情景。

您通常轮询源，这些源由从脉冲中提取的指示器组成。

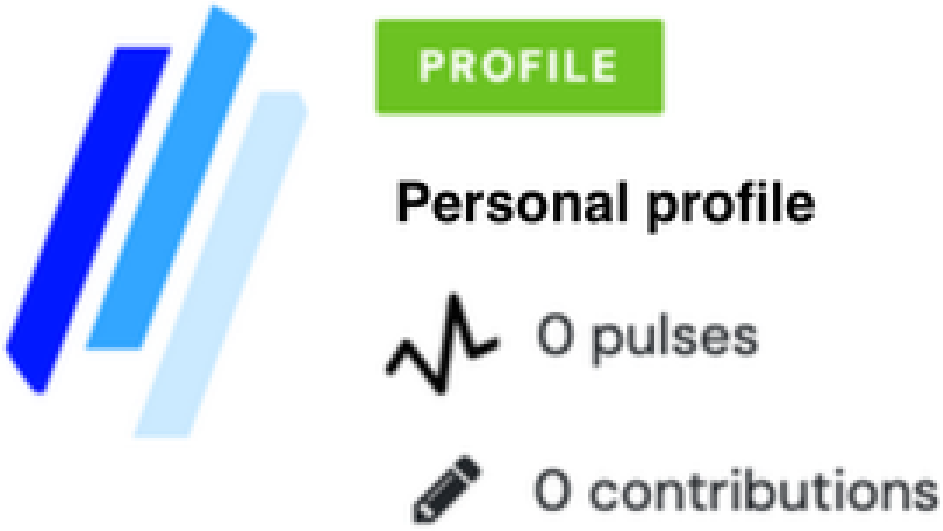
开始轮询收集

从自己的配置文件轮询

拥有您的AlienVault帐户后，您可以开始使用taxii-collections和taxii-poll命令。

以下是此使用案例的以下命令：

在这种情况下，在AlienVault配置文件中，没有可用的脉冲，但作为测试，您可以使用taxii-poll命令轮询配置文件中的集合：



alienvault个人配置文件

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

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

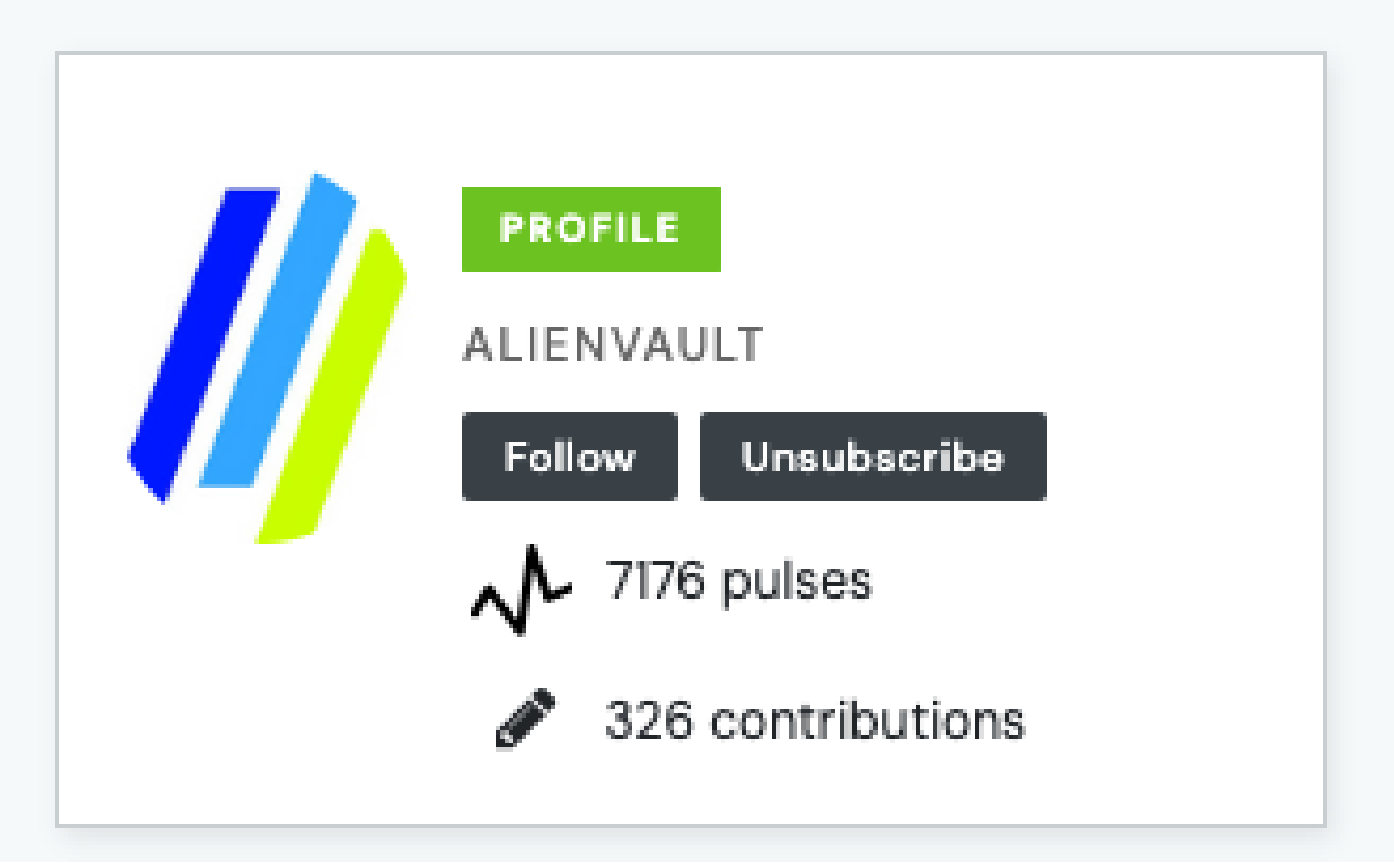
```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\
>     --username [redacted] --password [redacted]
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll
2025-05-27 12:13:41,51[redacted] INFO: 0 blocks polled
```

轮询个人配置文件

如您所见，AlienVault配置文件中没有可用的信息，因此没有轮询的块。

从AlienVault配置文件轮询

一旦发现AlienVault中的配置文件，其中一些配置文件会包含脉冲。在本示例中，使用AlienVault配置文件。



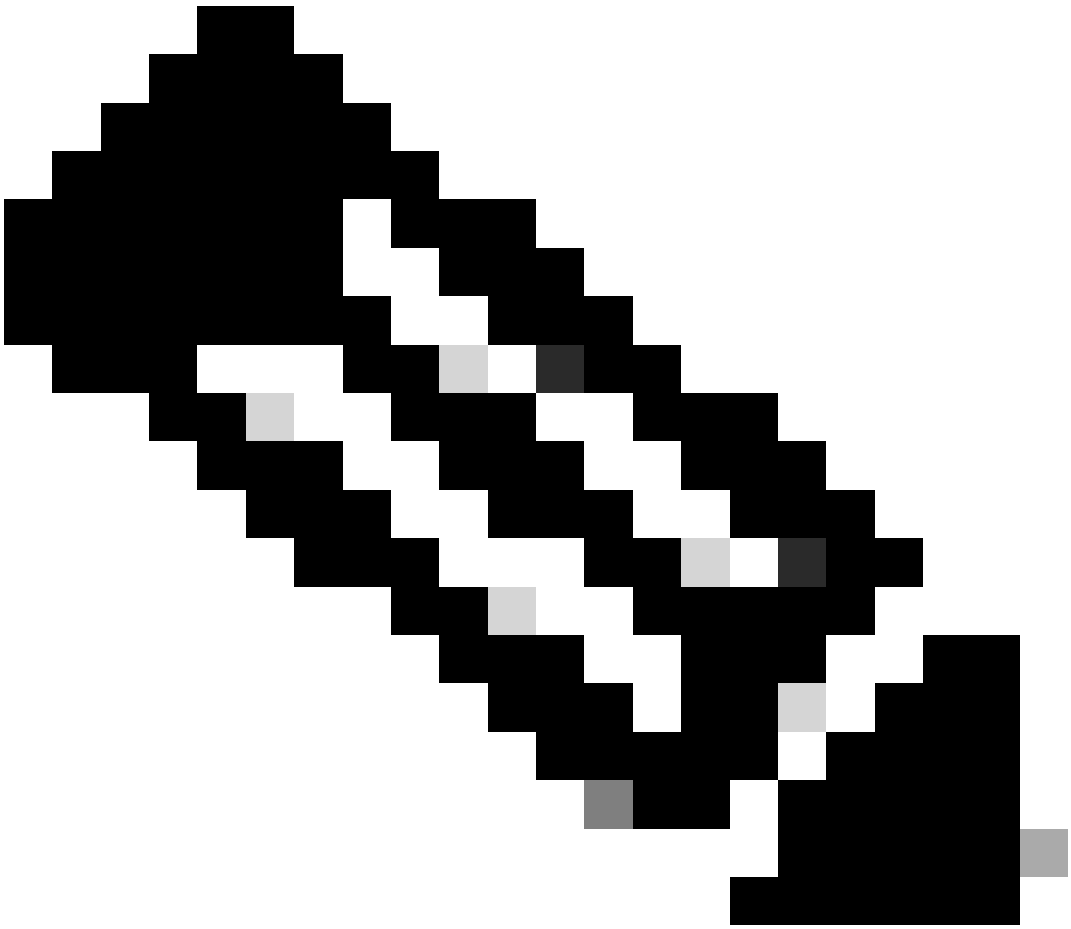
alienvault配置文件

使用taxii-poll命令运行轮询时，它会立即开始从配置文件中获取所有信息。

```
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:/
```

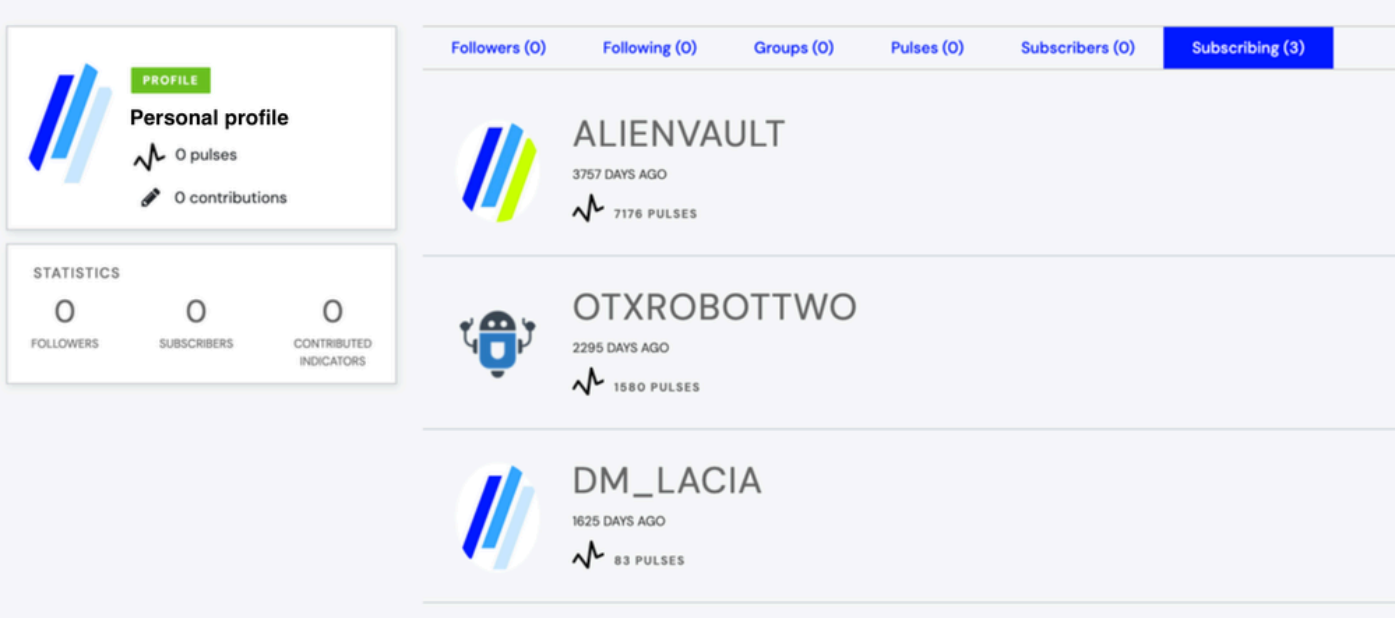
如图所示，流程开始获取信息。



注意：要了解您的用户名和密码，请选中此链接https://otx.alienvault.com/api

AlienVault配置文件集合订阅

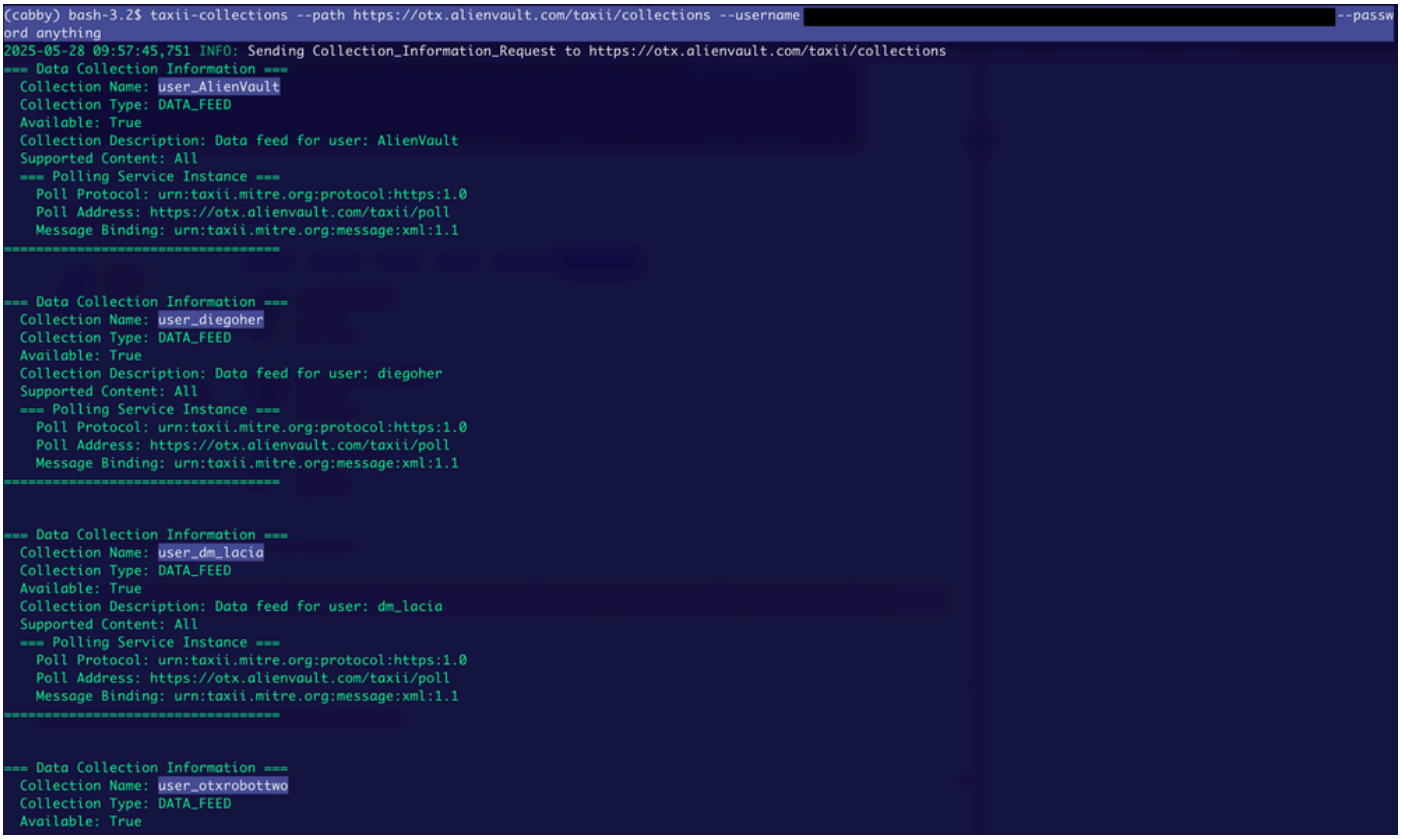
作为测试，此用户订用了3个配置文件。



个人简档订阅

您可以使用taxii-collections命令获取这些订阅。

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



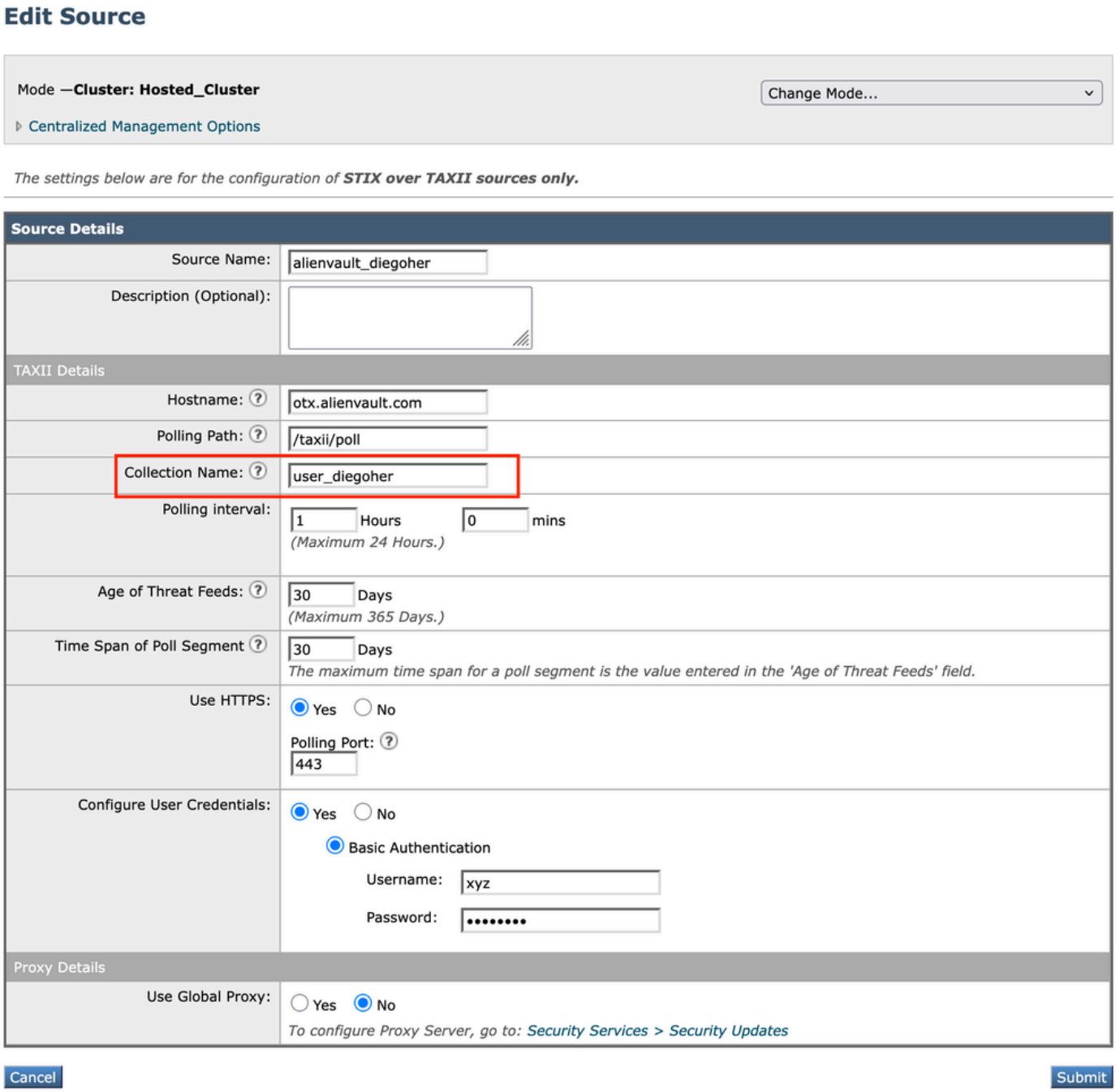
个人简档集合

如果“收集名称”(Collection Name)与您订用的名称相同，则可以确认taxii-collections命令是否有效。

将源添加到ESA

添加没有源的源

1. 导航到邮件策略 > 外部威胁源管理器。
2. 更改为集群模式。
3. 单击Add Source。
4. 主机名:otx.alienvault.com
5. 轮询路径：/taxi/poll
6. 集合名称：user_<your_AlienVault_username>
7. 端口：443
8. 配置用户凭证：AlienVault提供给你的那种。
9. 单击Submit > Commit Changes。



个人来源

无源的轮询源

在外部威胁源管理器中，添加源后，新添加的源将可见。

个人馈送

添加后，单击Poll Now。

验证

通过CLI登录ESA并查看威胁源日志以验证信息。

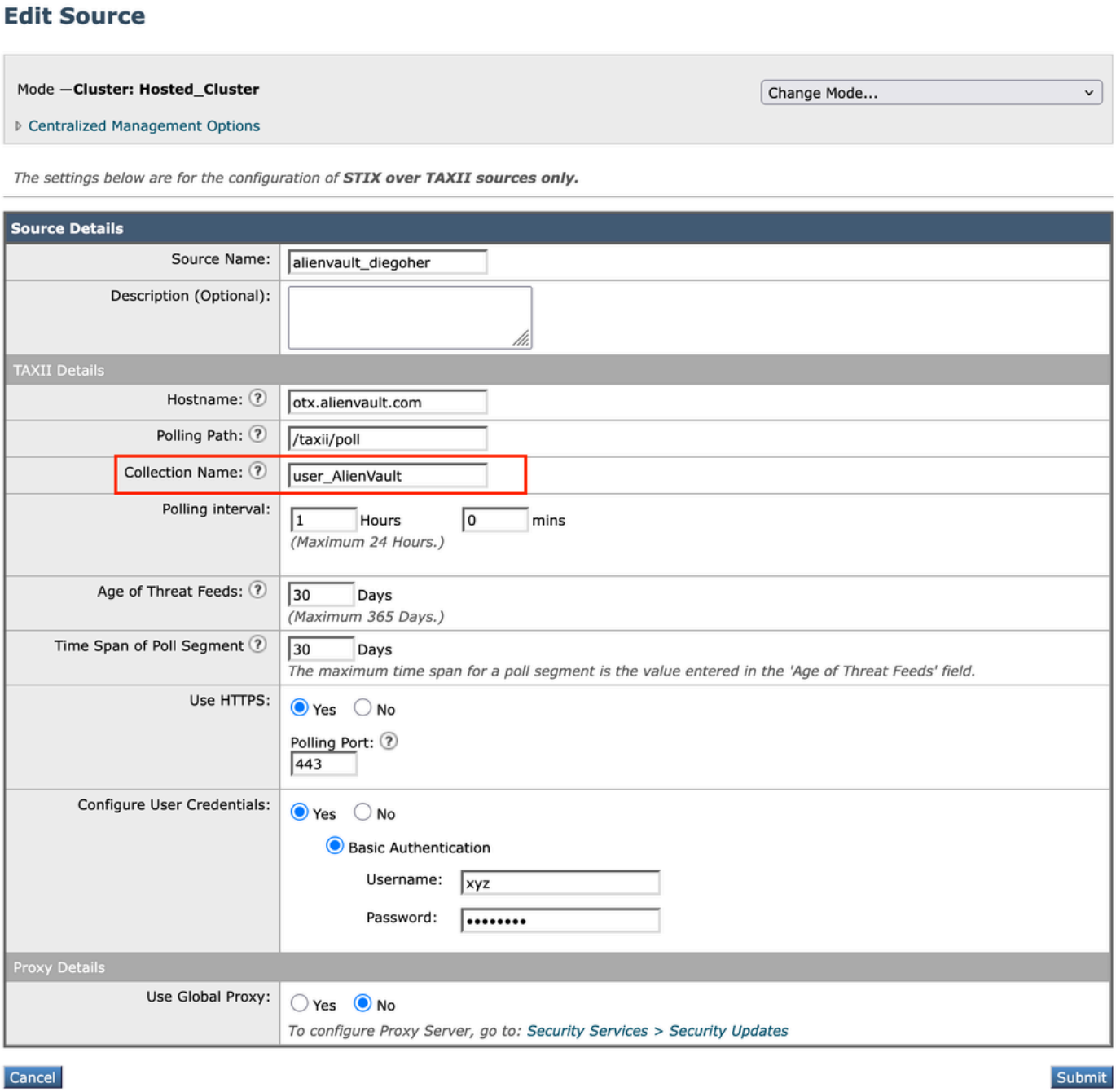
```
THREAT_FEEDS: A delta poll is scheduled for the source: alienvault_diegoher
THREAT_FEEDS: A delta poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_diegoher
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-06-10 10:22:33.058477 and 2025-06-10

THREAT_FEEDS: No new observables were fetched from the source: alienvault_diegoher
THREAT_FEEDS: 0 observables were fetched from the source: alienvault_diegoher
```

ETF个人调查

如图所示，您可以看到提取了0个可观察量，这是预期结果，因为显示的配置文件中没有源。

添加源与源

1. 导航到邮件策略 > 外部威胁源管理器。
2. 更改为集群模式。
3. 单击Add Source。
4. 主机名:otx.alienvault.com
5. 轮询路径：/taxi/poll
6. 集合名称：user_AlienVault
7. 端口：443
8. 配置用户凭证：AlienVault提供给你的那种。
9. 单击Submit > Commit Changes。



Alienvault源

具有源的轮询源

在外部威胁源管理器中，添加源后，新添加的源将可见。

alienvault馈送

添加后，点击Poll Now。

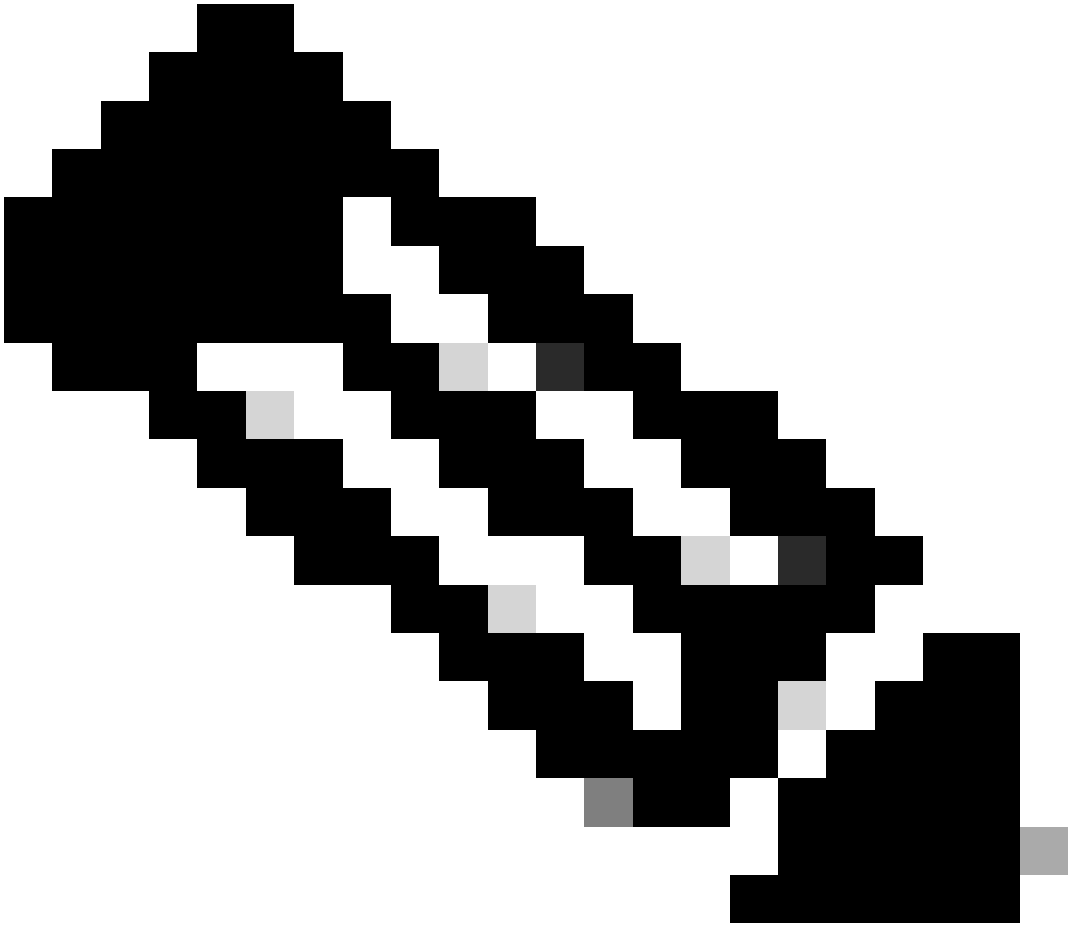
验证

通过CLI登录ESA并查看威胁源日志以验证信息。

```
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
```

轮询alienvault源

如图所示，您可以看到读取了几个观察值。



注意：如果向配置的集合中添加了新源，ESA将自动轮询源，并获取新的可观察量。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。