將AlienVault配置為ESA的外部威脅源

目錄

簡介

本文檔介紹從AlienVault源配置外部威脅源並在ESA中使用它的步驟。

必要條件

需求

思科建議瞭解以下主題：

- 思科安全電子郵件閘道(SEG/ESA)AsyncOS 16.0.2
- Linux CLI

- Python3 pip
- AlienVault帳戶

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 電子郵件安全裝置
- Python3

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

外部威脅源(ETF)框架使郵件網關能夠通過TAXII協定接收以STIX格式共用的外部威脅情報。通過利用此功能，組織可以：

- 主動應對惡意軟體、勒索軟體、網路釣魚和針對性攻擊等網路威脅。
- 訂閱本地和第三方威脅情報源。
- 增強電子郵件網關的整體有效性。

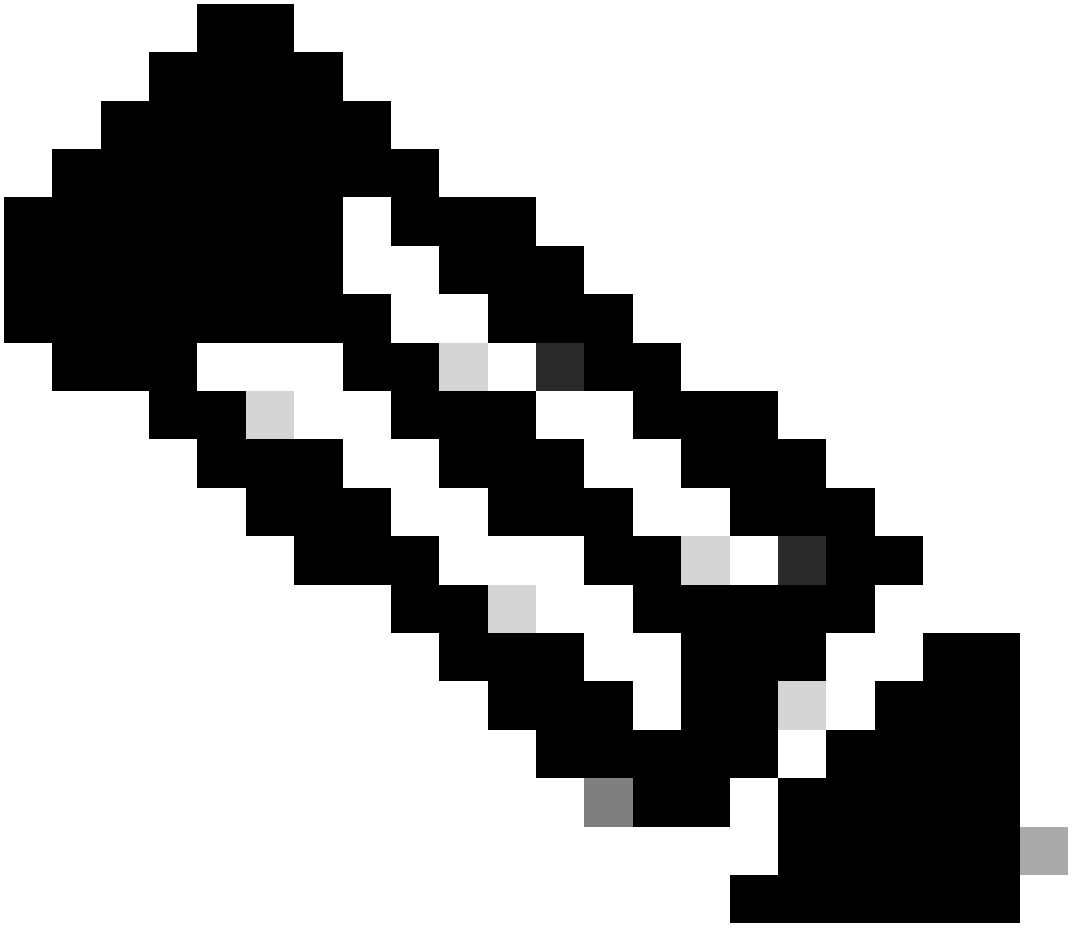
什麼是STIX/TAXII?

STIX（結構化威脅資訊表達）

STIX是一種標準化格式，用於以結構化和機器可讀的方式描述網路威脅情報(CTI)，包括指標、戰術、技術、惡意軟體和威脅實施者。STIX饋送通常包括指示符 — 有助於檢測可疑或惡意網路活動的模式。

TAXII（可信的自動情報資訊交換）

TAXII是一種用於在系統之間安全、自動地交換STIX資料的協定。定義如何在系統、產品或組織之間通過專用服務（TAXII伺服器）交換網路威脅情報。



註:AsyncOS 16.0版本支援STIX/TAXII版本：STIX 1.1.1和1.2,TAXII 1.1。

源源

郵件安全裝置可以使用來自各種來源的威脅情報源，包括公共儲存庫、商業提供商以及您組織內他們自己的專用伺服器。

為確保相容性，所有來源都必須使用STIX/TAXII標準，這些標準支援威脅資料的結構化、自動共用。

Cabby庫

Cabby Python庫是連線到TAXII伺服器、發現STIX集合和輪詢威脅資料的有用工具。在將資料來源整合到您的郵件安全裝置之前，這是一個測試和驗證資料來源是否正常工作以及是否按預期返回資

料的好方法。

安裝Cabby庫

要安裝Cabby庫，您需要確保本地電腦已安裝Python pip。

安裝python pip後，只需運行此命令即可安裝cabby庫。

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

完成cabby庫安裝後，您可以驗證taxii-collections和taxii-poll命令現在是否可用。

```
(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 — 脈衝和饋送

若要開始發現AlienVault資訊，請先在AlienVault站點上建立帳戶，然後開始搜尋所需的資訊。

在AlienVault中，源和脈衝是相關的，但不相同：

脈衝

脈衝是帶有分組指示符+情景的威脅英特爾（人可讀）。

- Pulse是圍繞特定威脅或活動進行分組的威脅指標(IOC)的集合。
- 由社群或提供商建立，用於描述諸如惡意軟體、網路釣魚、勒索軟體之類的內容。
- 每個脈衝都包括威脅描述、相關指標（IP、域、檔案雜湊等）、標籤和引用等上下文。
- 脈衝是人類可讀的，其結構方式易於理解和共用。

將脈衝視為具有分組IOC和後設資料的威脅報告。

源

供給是來自多個脈衝的自動指示符流（機器可讀）。

- 源是指從一個或多個脈衝提取的原始指示符(IOC)流，通常以自動方式提取。
- 安全工具通常使用它們通過STIX/TAXII、CSV或JSON等格式批次接收指標。
- 訂閱源以電腦為中心，用於自動化和與SIEM、防火牆和電子郵件網關的整合。

饋送更多的是關於傳遞機制，而脈衝則是威脅的內容和情景。

您通常輪詢源，這些源由從脈衝中提取的指示器組成。

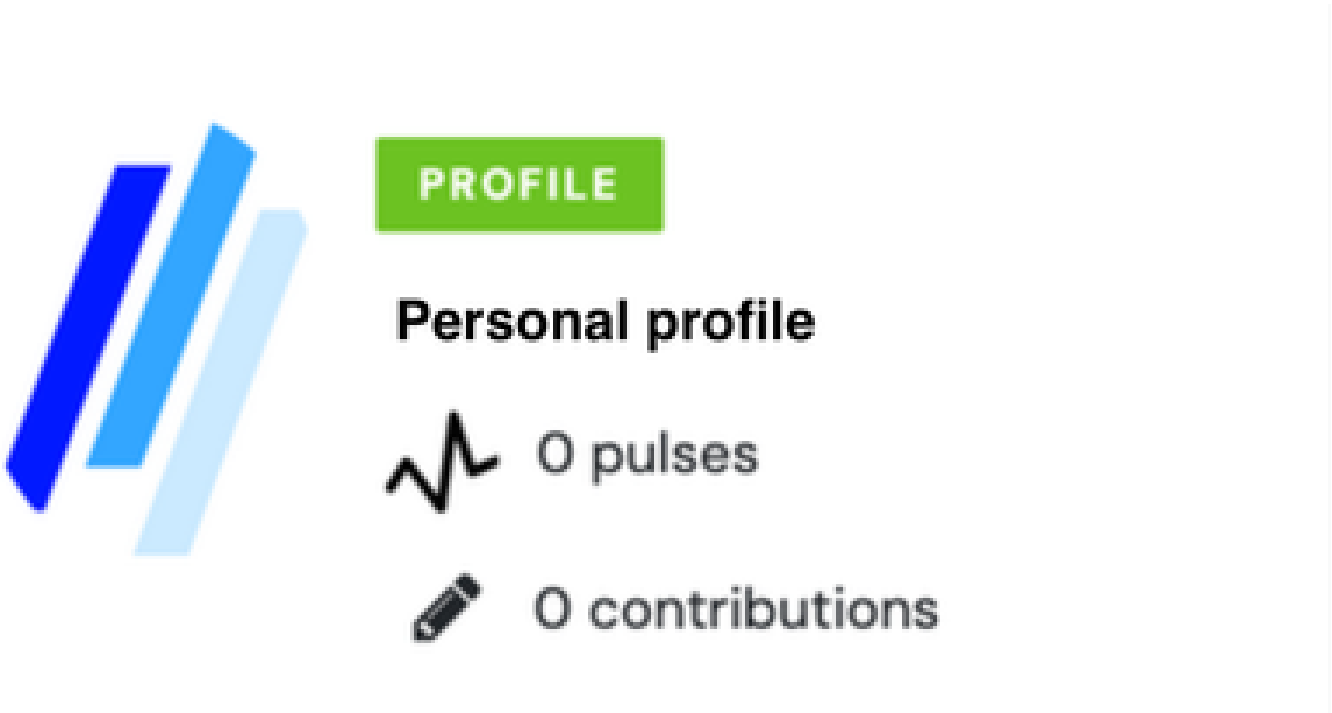
開始輪詢集合

從自己的配置檔案輪詢

擁有AlienVault帳戶後，可以開始使用taxii-collections和taxii-poll 命令。

以下是此使用案例中使用這些命令的方式：

在這種情況下，在AlienVault配置檔案中，沒有可用的脈衝，但作為測試，您可以使用taxii-poll命令輪詢配置檔案中的集合：



alienvault個人配置檔案

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

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

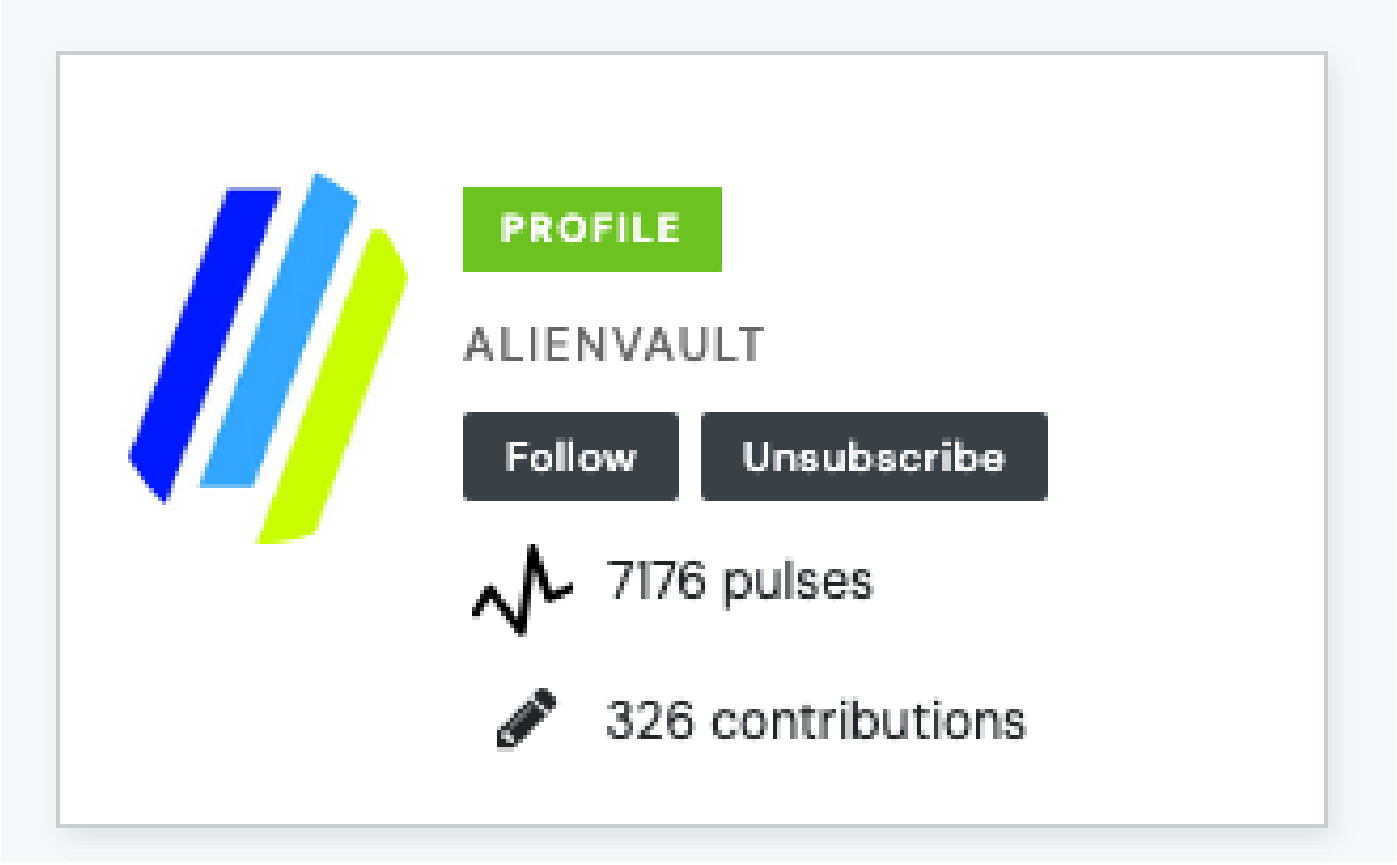
```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\
>     --username [redacted] --password [redacted]
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll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

投票個人配置檔案

您可以看到，由於在AlienVault配置檔案中沒有可用的資訊，因此沒有輪詢的塊。

從AlienVault配置檔案輪詢

一旦發現AlienVault中的配置檔案，其中一些會有脈衝。在本示例中，使用AlienVault配置檔案。



alienvault配置檔案

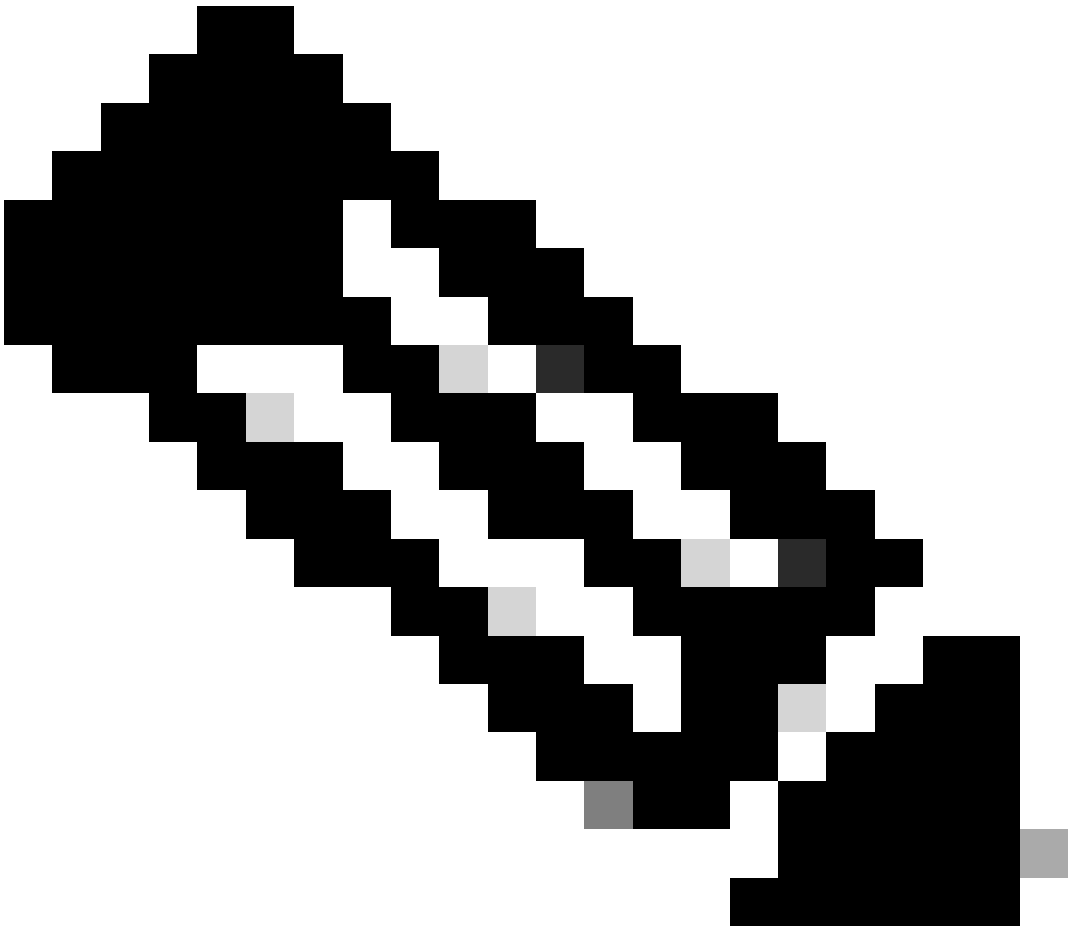
使用taxii-poll命令運行輪詢時，它立即開始從配置檔案中獲取所有資訊。

```
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                                                    --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調查

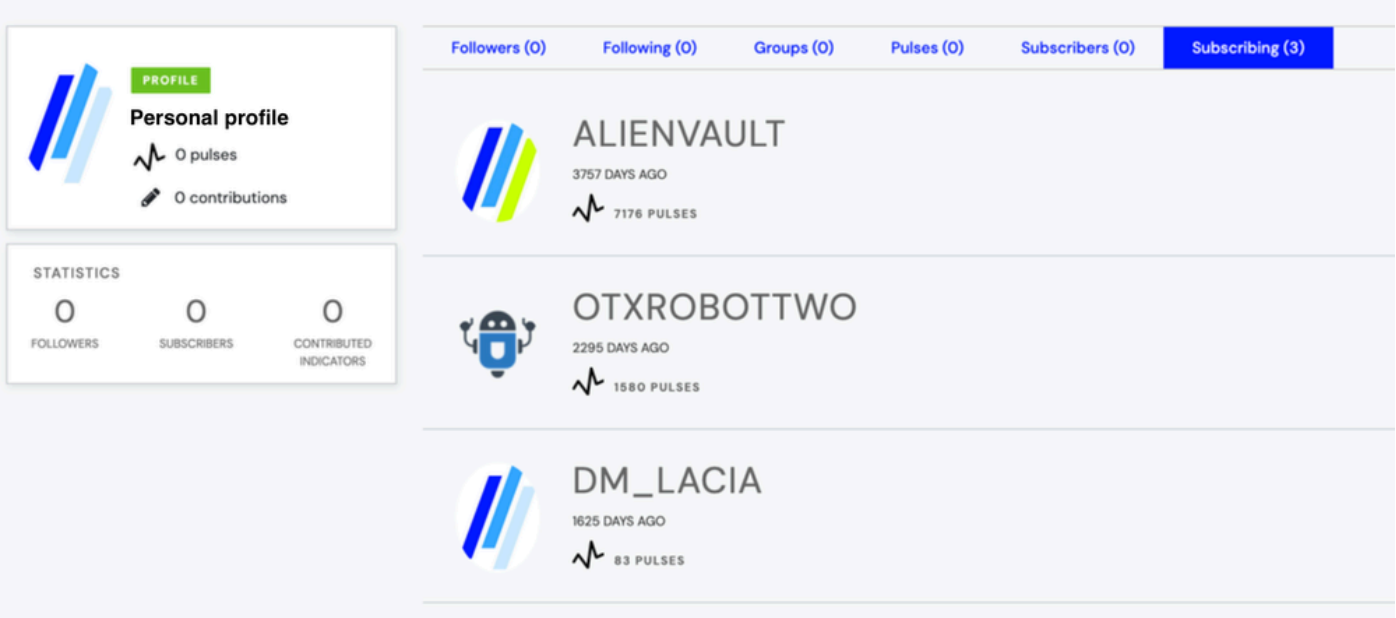
如圖所示，進程開始獲取資訊。



附註：要瞭解您的使用者名稱和密碼，請選中此連結https://otx.alienvault.com/api

AlienVault配置檔案集合訂閱

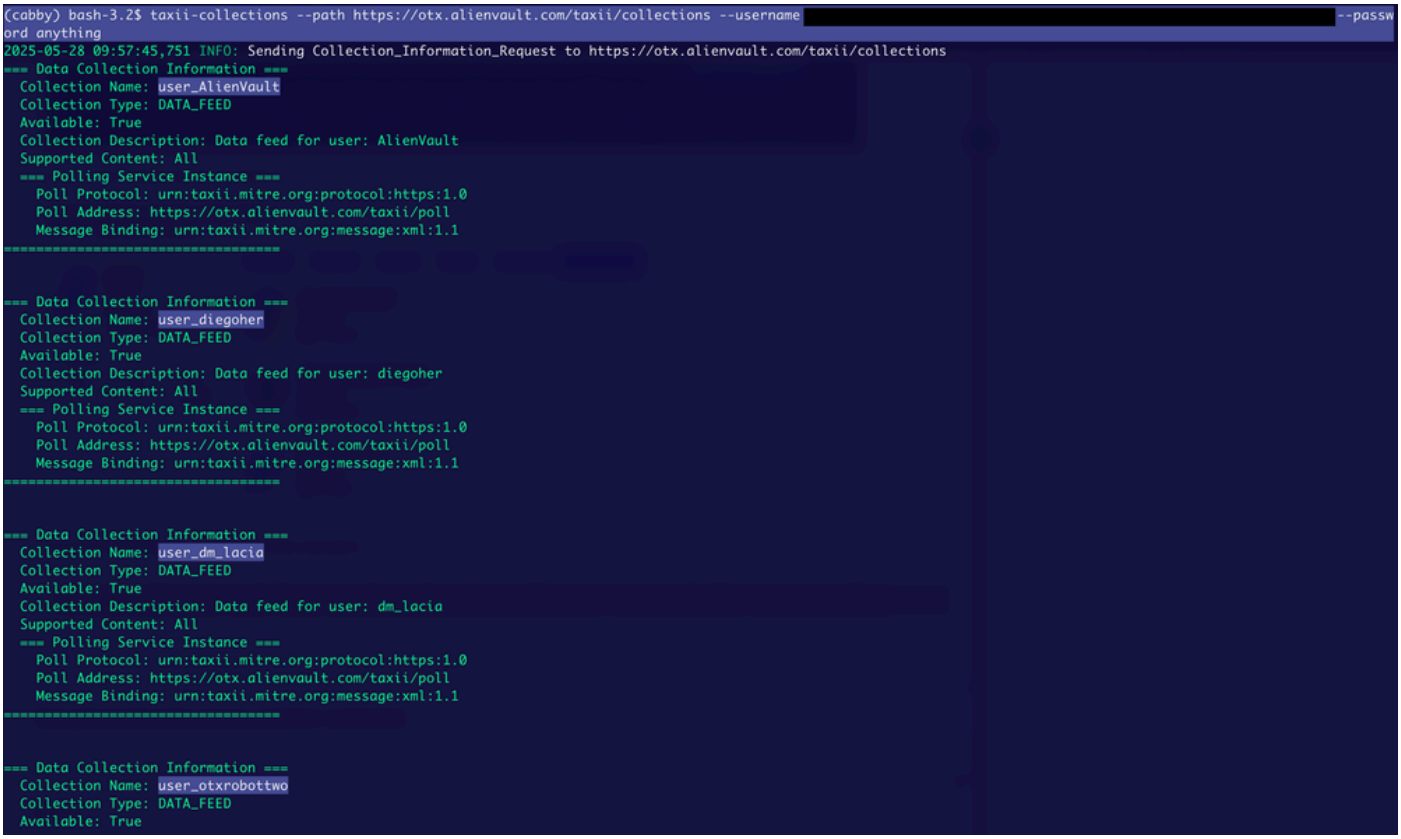
作為測試，此使用者訂閱了3個配置檔案。



個人配置檔案訂閱

您可以使用taxii-collections 命令獲取這些訂閱。

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



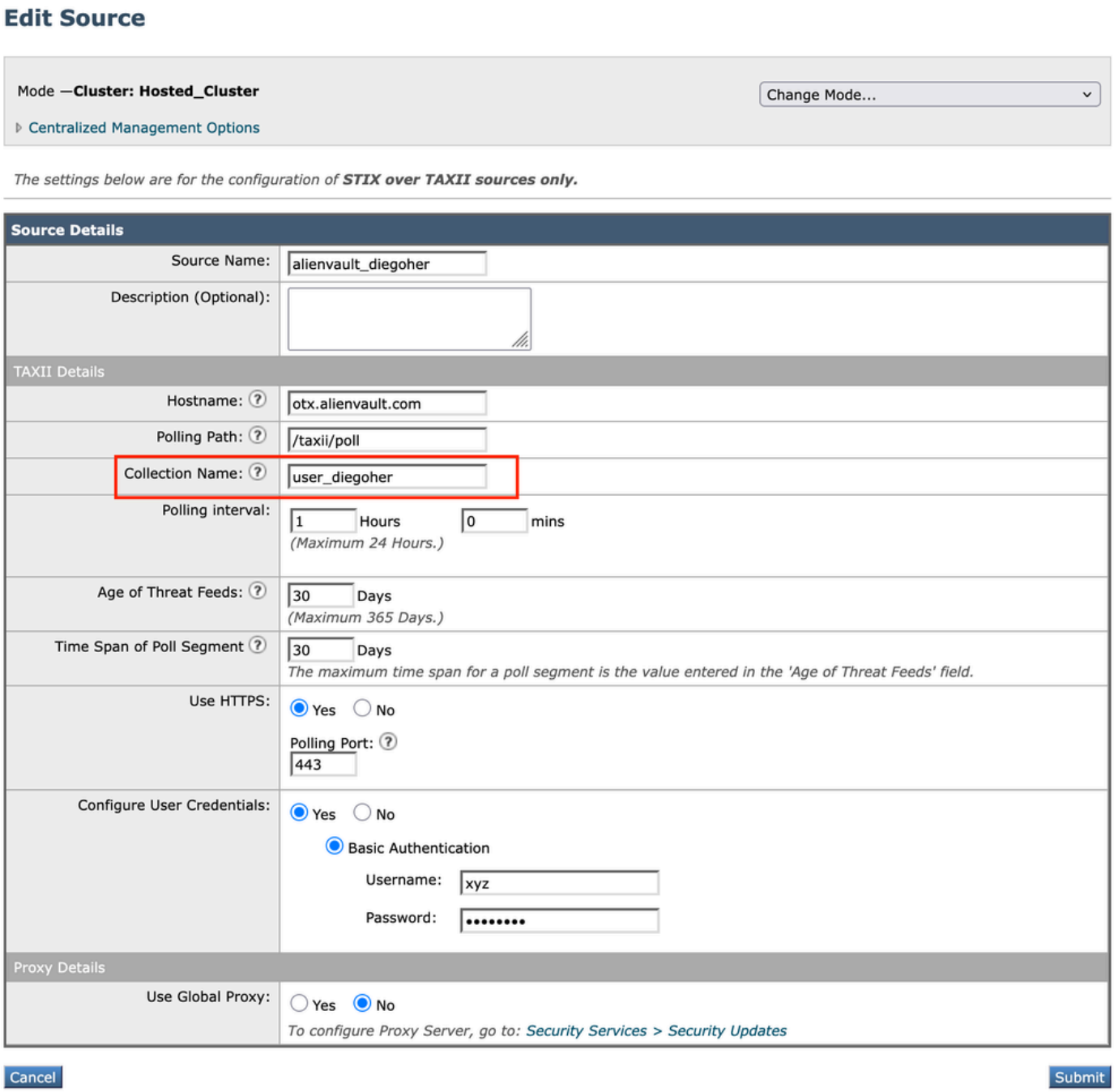
個人配置檔案集合

如果「集合名稱」與您訂閱的集合名稱相同，則可以確認taxii-collections命令是否有效。

將源新增到ESA

新增沒有源的源

1. 導航到Mail Policies > External Threat Feed Manager。
2. 更改為集群模式。
3. 按一下「Add Source」。
4. 主機名：otx.alienvault.com
5. 輪詢路徑：/taxi/poll
6. 集合名稱：user_<your_AlienVault_username>
7. 連接埠：443
8. 配置使用者憑據：是AlienVault提供給您的產品。
9. 點選提交 > 提交更改。



個人來源

無源的輪詢源

在外部威脅源管理器中，新增源後，新新增的源將可見。

個人饋送

新增後，按一下Poll Now。

驗證

通過CLI登入到ESA並檢視威脅源日誌以驗證資訊。

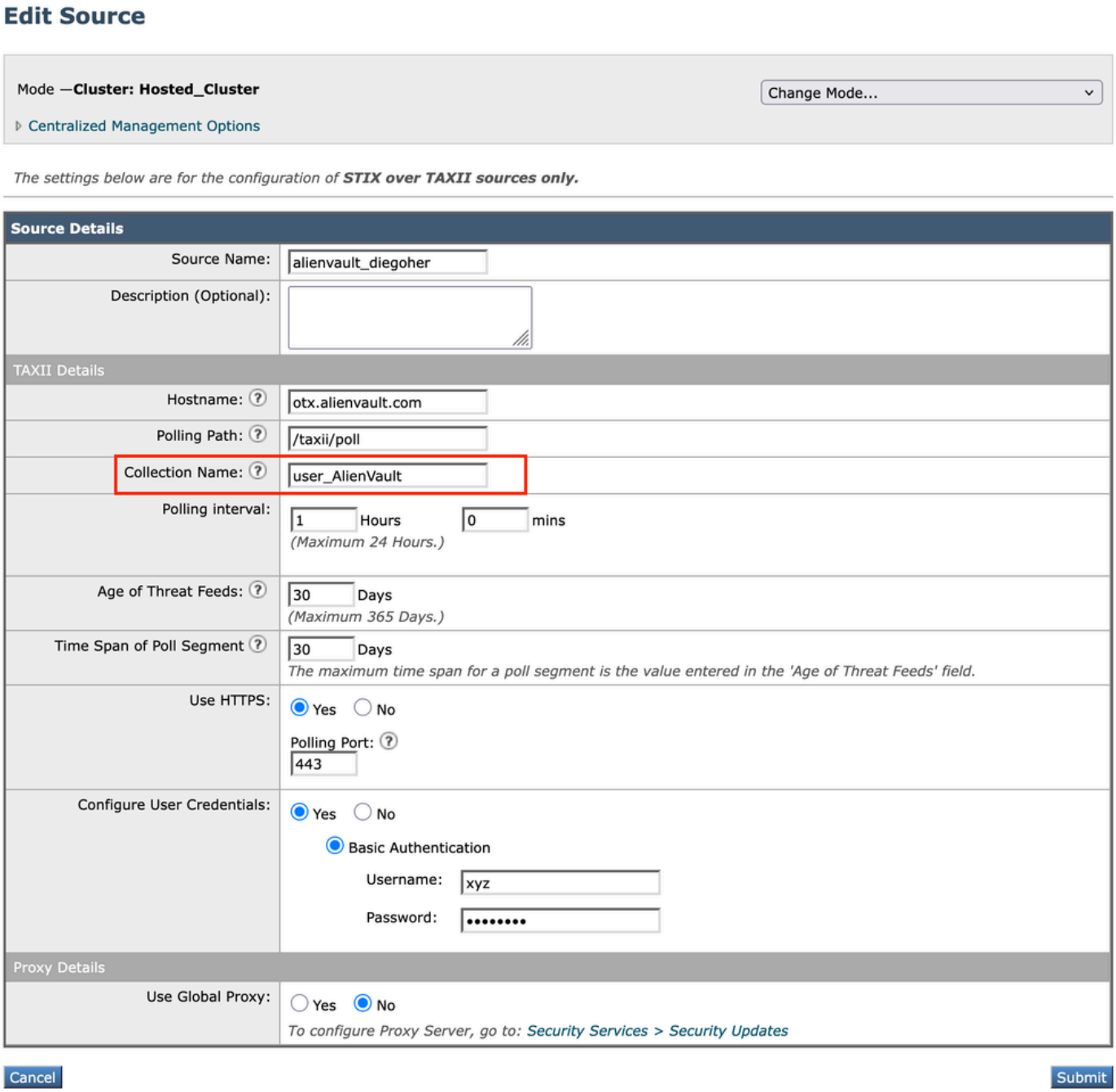
```
THREAT_FEEDS: A delta poll is scheduled for the source: alienvault_diegoher
THREAT_FEEDS: A delta poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_diegoher
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-06-10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

如圖所示，您可以看到讀取了0個可觀察量，這是預期的，因為圖中所示的簡檔中沒有饋送。

新增源與源

1. 導航到Mail Policies > External Threat Feed Manager。
2. 更改為集群模式。
3. 按一下「Add Source」。
4. 主機名：otx.alienvault.com
5. 輪詢路徑：/taxi/poll
6. 集合名稱：user_AlienVault
7. 連接埠：443
8. 配置使用者憑據：是AlienVault提供給您的產品。
9. 點選提交 > 提交更改。



alienvault源

具有源的輪詢源

在外部威脅源管理器中，新增源後，新新增的源將可見。

alienvault饋送

新增後，按一下Poll Now。

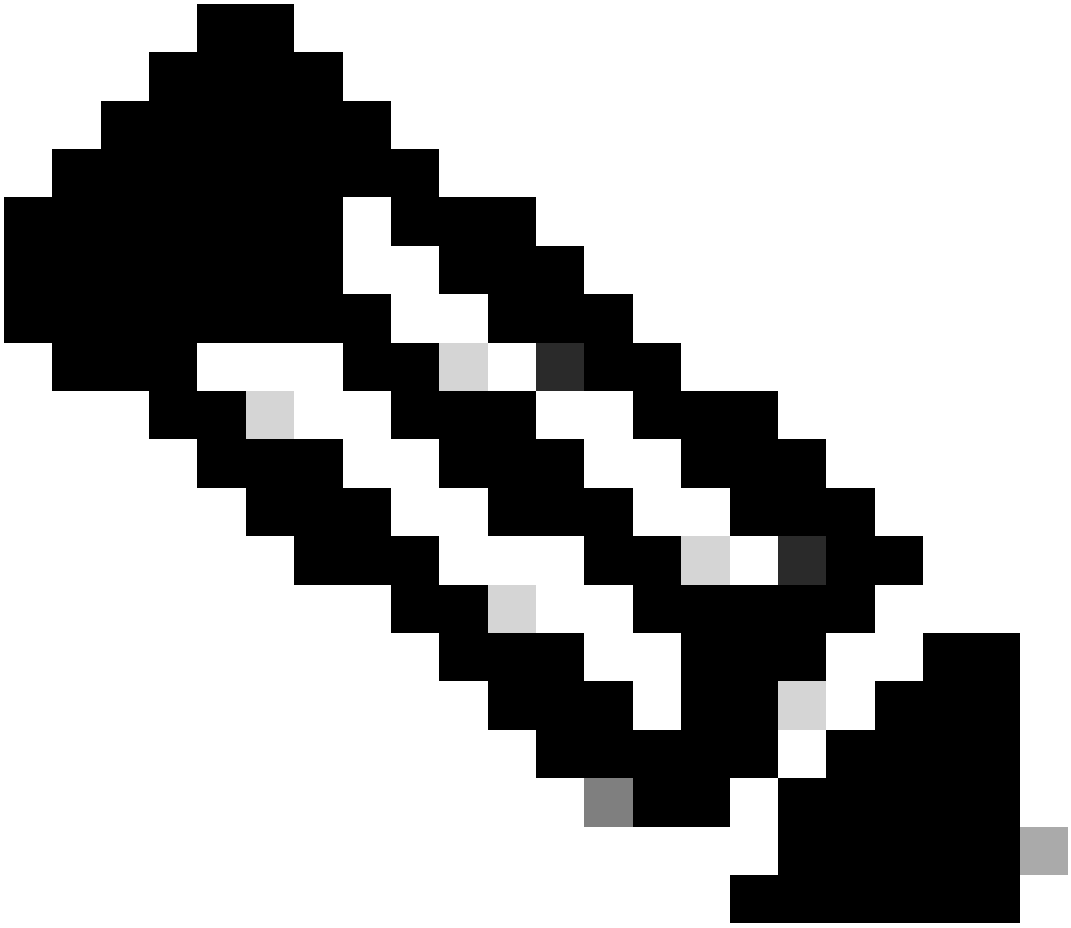
驗證

通過CLI登入到ESA並檢視威脅源日誌以驗證資訊。

```
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
```

輪詢alienvault源

如圖所示，您可以看到讀取了多個可觀察量。



附註：如果向已配置的集合中新增新源，則ESA會自動輪詢源，並獲取新的可觀察量。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。