

ESAの外部脅威フィードとしてのAlienVaultの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[STIX/TAXIIとは](#)

[STIX\(Structured Threat Information Expression\)](#)

[TAXII\(Trusted Automated Exchange of Intelligence Information\)](#)

[フィードソース](#)

[キャビー図書館](#)

[Cabbyライブラリのインストール](#)

[AlienVault – バルスとフィード](#)

[バルス](#)

[フィード](#)

[ポーリングコレクションの開始](#)

[自分のプロファイルからのポーリング](#)

[AlienVaultプロファイルからのポーリング](#)

[AlienVaultプロファイルコレクションサブスクリプション](#)

[ESAへの送信元の追加](#)

[フィードなしのソースの追加](#)

[フィードなしのポーリングソース](#)

[確認](#)

[フィードを使用したソースの追加](#)

[フィードを使用したソースのポーリング](#)

[確認](#)

はじめに

このドキュメントでは、AlienVaultソースから外部脅威フィードを設定し、ESA内で使用する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Email Gateway(SEG/ESA)AsyncOS 16.0.2
- LinuxのCLI
- Python3のPIP
- AlienVaultアカウント

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Eメールセキュリティ アプライアンス
- Python3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

外部脅威フィード(ETF)フレームワークを使用すると、Eメールゲートウェイは、TAXIIプロトコルを介してSTIX形式で共有される外部脅威インテリジェンスを取り込むことができます。この機能を活用することで、組織は次のことが可能になります。

- マルウェア、ランサムウェア、フィッシング、標的型攻撃などのサイバー脅威に対して積極的に対応します。
- ローカルとサードパーティの両方の脅威インテリジェンスソースを購読します。
- Eメールゲートウェイの全体的な効率を向上させます。

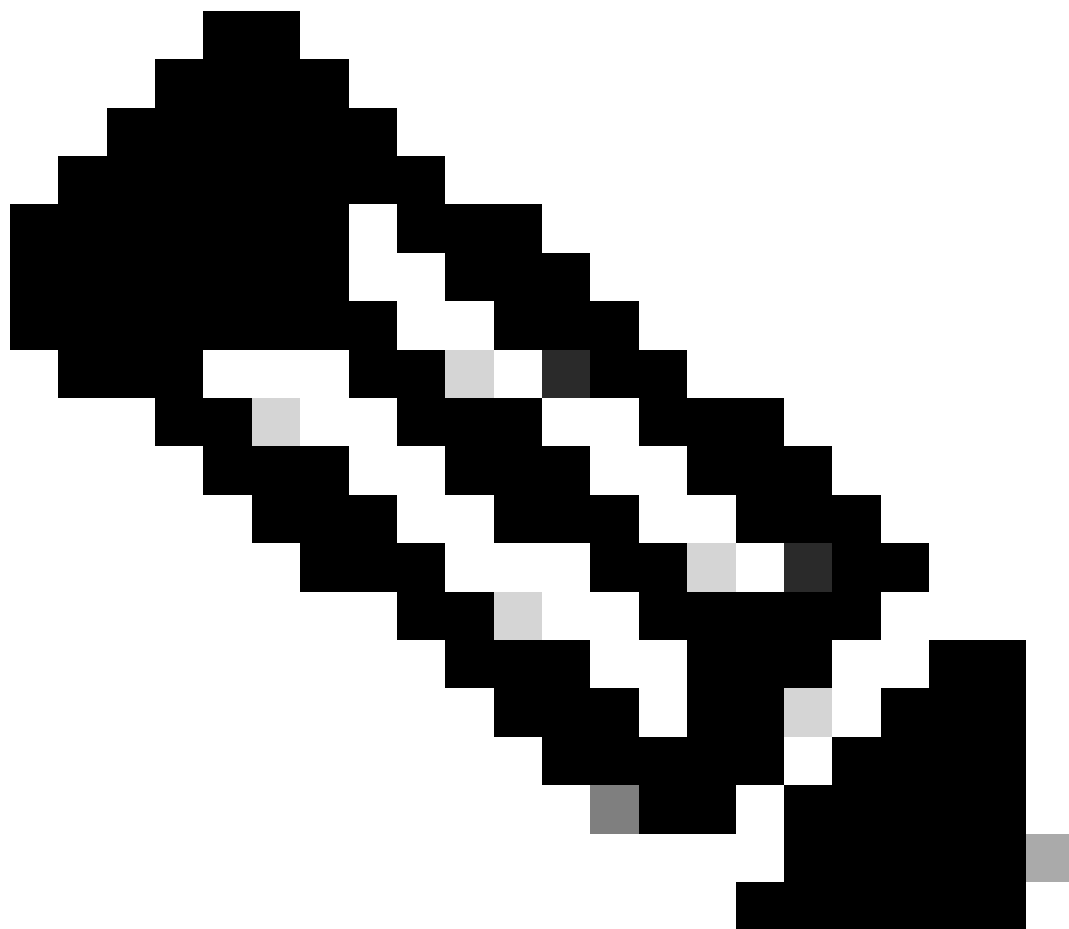
STIXX/TAXIIとは

STIX(Structured Threat Information Expression)

STIXは、サイバー脅威インテリジェンス(CTI)を構造化された機械が読める方法で記述するために使用される標準化された形式です。CTIには、インジケータ、戦術、手法、マルウェア、脅威アクターなどが含まれます。STIXフィードには通常、疑わしいサイバー活動や悪意のあるサイバー活動の検出に役立つパターンなどのインジケータが含まれます。

TAXII(Trusted Automated Exchange of Intelligence Information)

TAXIIは、システム間でSTIXデータを安全かつ自動的に交換するために使用されるプロトコルです。専用サービス (TAXIIサーバ) を通じて、システム、製品、または組織間でサイバー脅威インテリジェンスを交換する方法を定義します。



注:AsyncOS 16.0リリースはSTIX/TAXIIバージョン (STIX 1.1.1および1.2、TAXII 1.1) をサポートします。

フィードソース

Eメールセキュリティアプライアンスは、パブリックリポジトリ、商用プロバイダー、組織内の独自のプライベートサーバなど、さまざまなソースからの脅威インテリジェンスフィードを利用できます。

互換性を確保するため、すべてのソースはSTIX/TAXII標準を使用する必要があります。この標準により、脅威データの構造化された自動共有が可能になります。

キャビー図書館

Cabby Pythonライブラリは、TAXIIサーバへの接続、STIXコレクションの検出、および脅威データのポーリングに便利なツールです。これは、フィードソースが正常に動作していることをテストおよび検証し、Eメールセキュリティアプライアンスに統合する前にデータを期待どおりに返す優れた方法です。

Cabbyライブラリのインストール

Cabbyライブラリをインストールするには、ローカルマシンにPython pipがインストールされていることを確認する必要があります。

python pipをインストールしたら、このコマンドを実行してcabbyライブラリをインストールするだけです。

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

cabbyライブラリのインストールが完了すると、taxii-collectionsコマンドとtaxii-pollコマンドが使用可能になったことを確認できます。

```
(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] [--verbose]
                 [--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 – パルスとフィード

AlienVault情報の検出を開始するには、まずAlienVaultサイトでアカウントを作成し、次に目的の情報の検索を開始します。

AlienVaultでは、フィードとパルスは関連していますが、同じではありません。

パルス

パルスは、グループ化されたインジケータ+コンテキスト（人間が読み取り可能）を備えた脅威intelによってキュレートされます。

- Pulseは、特定の脅威またはキャンペーンを中心にグループ化された脅威インジケータ (IOC)の集合です。
- マルウェア、フィッシング、ランサムウェアなどを記述するためにコミュニティまたはプロバイダーによって作成されます。
- 各パルスには、脅威の説明、関連するインジケータ (IP、ドメイン、ファイルハッシュなど)、タグ、参照などのコンテキストが含まれます。
- パルスは人間が読んで理解し、共有しやすい方法で構成されます。

パルスは、グループ化されたIOCとメタデータを含む脅威レポートと考えてください。

フィード

フィードは、複数のパルスからのインジケータの自動ストリームです (機械読み取り可能)。

- フィードは、通常は自動化された方法で、1つ以上のパルスから抽出される生のインジケータ (IOC)のストリームです。
- 通常、セキュリティツールで使用され、STIX/TAXII、CSV、またはJSONなどの形式でインジケータを一括して取り込みます。
- フィードはマシンに重点を置いており、SIEM、ファイアウォール、Eメールゲートウェイとの自動化および統合に使用されます。

フィードは配信メカニズムに関するものですが、パルスは脅威の内容とコンテキストです。

フィードのポーリングは通常、パルスから抽出されたインジケータで構成されます。

ポーリングコレクションの開始

自分のプロファイルからのポーリング

AlienVaultアカウントを作成したら、taxii-collectionsコマンドとtaxii-pollコマンドの使用を開始できます。

次に、この使用例でこれらのコマンドを使用する方法を示します。

この場合、AlienVaultプロファイル内には使用可能なパルスはありませんが、テストとして、taxii-pollコマンドを使用してプロファイルからコレクションをポーリングできます。



PROFILE

Personal profile



0 pulses



0 contributions

alienvault/パーソナルプロフィール

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

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

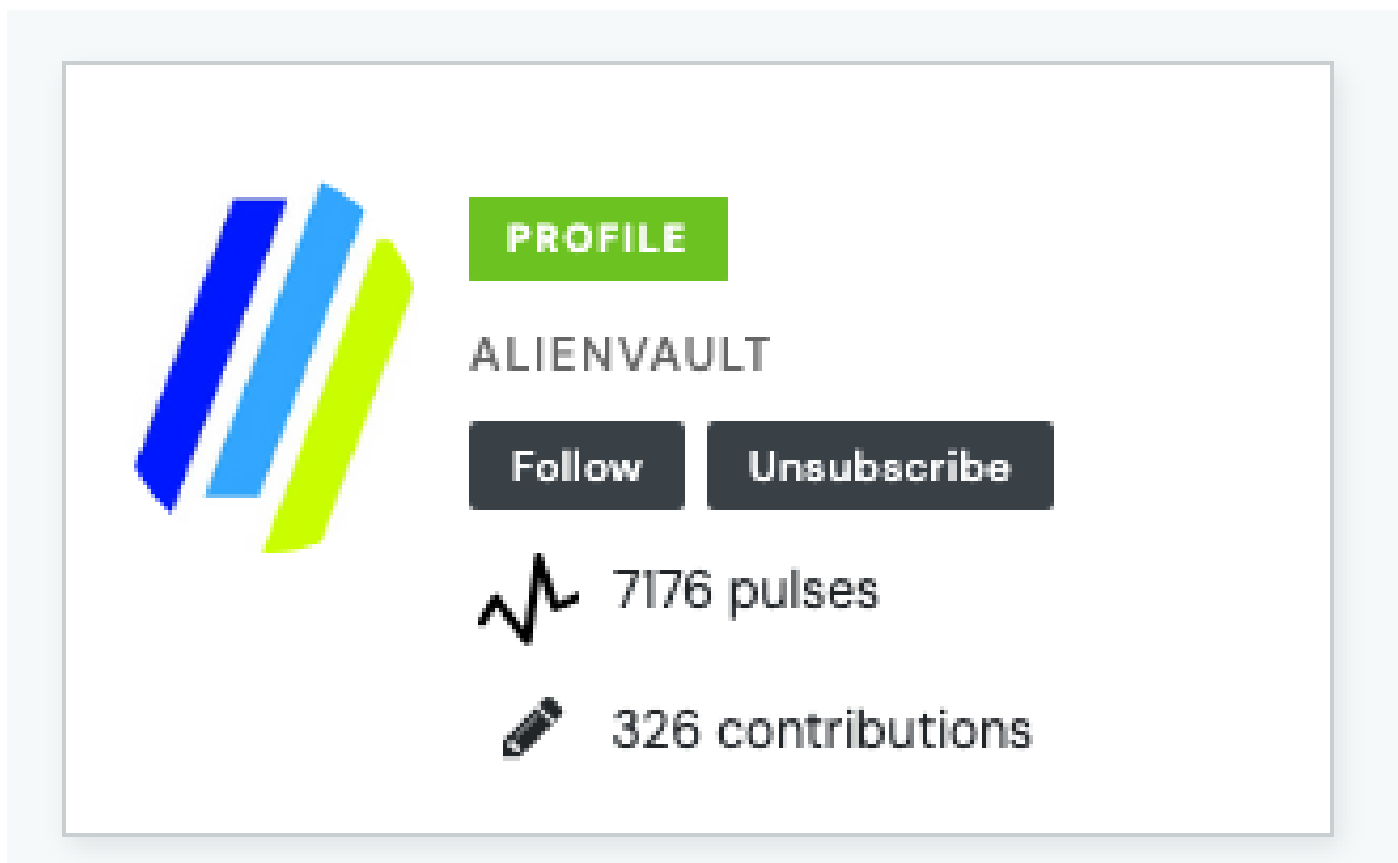
```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\
> --username [REDACTED] --password [REDACTED]
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll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

ポーリング個人プロフィール

AlienVaultプロフィール内に使用可能な情報がないため、ポーリングされたブロックはありません。

AlienVaultプロフィールからのポーリング

AlienVault内のプロフィールが検出されると、一部のプロフィールにパルスが生成されます。この例では、AlienVaultプロフィールを使用します。



alienvaultプロフィール

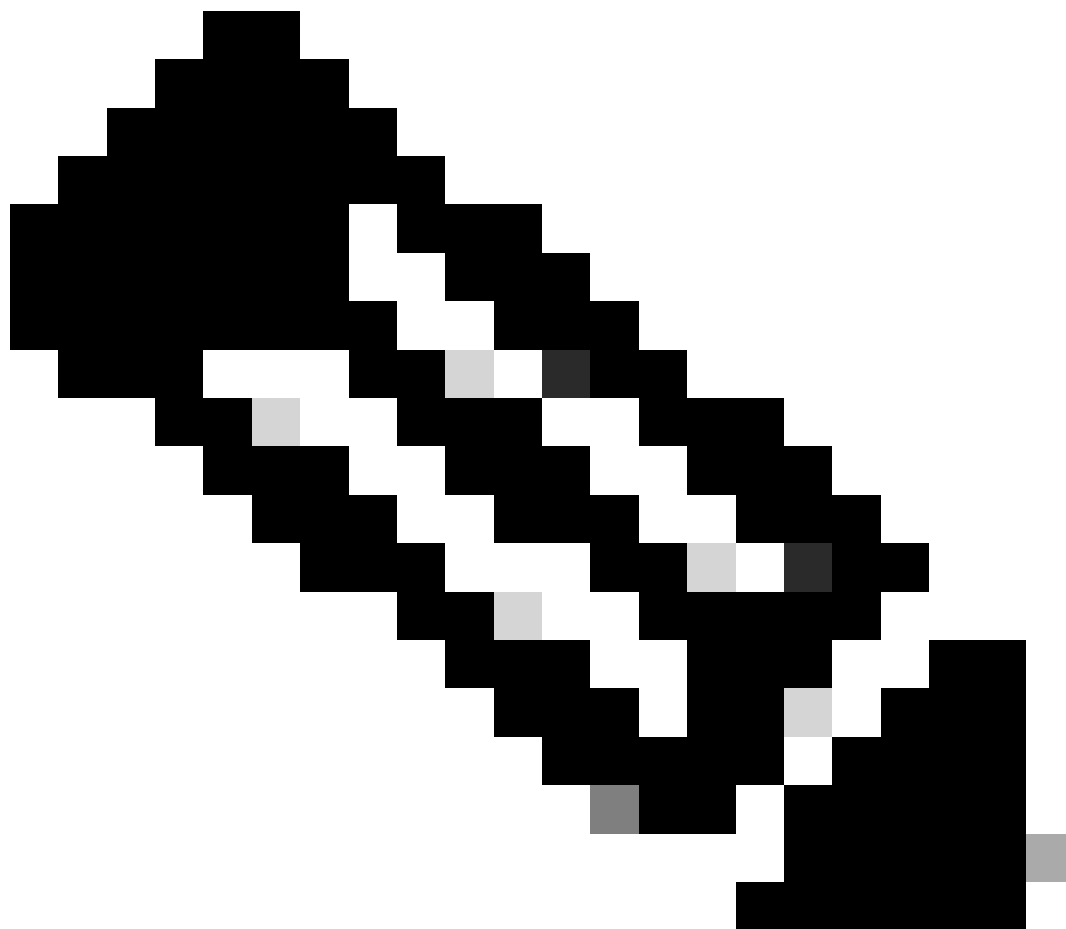
taxii-pollコマンドによるポーリングを実行すると、プロフィールからすべての情報のフェッチが即時に開始されます。

```
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ポーリング

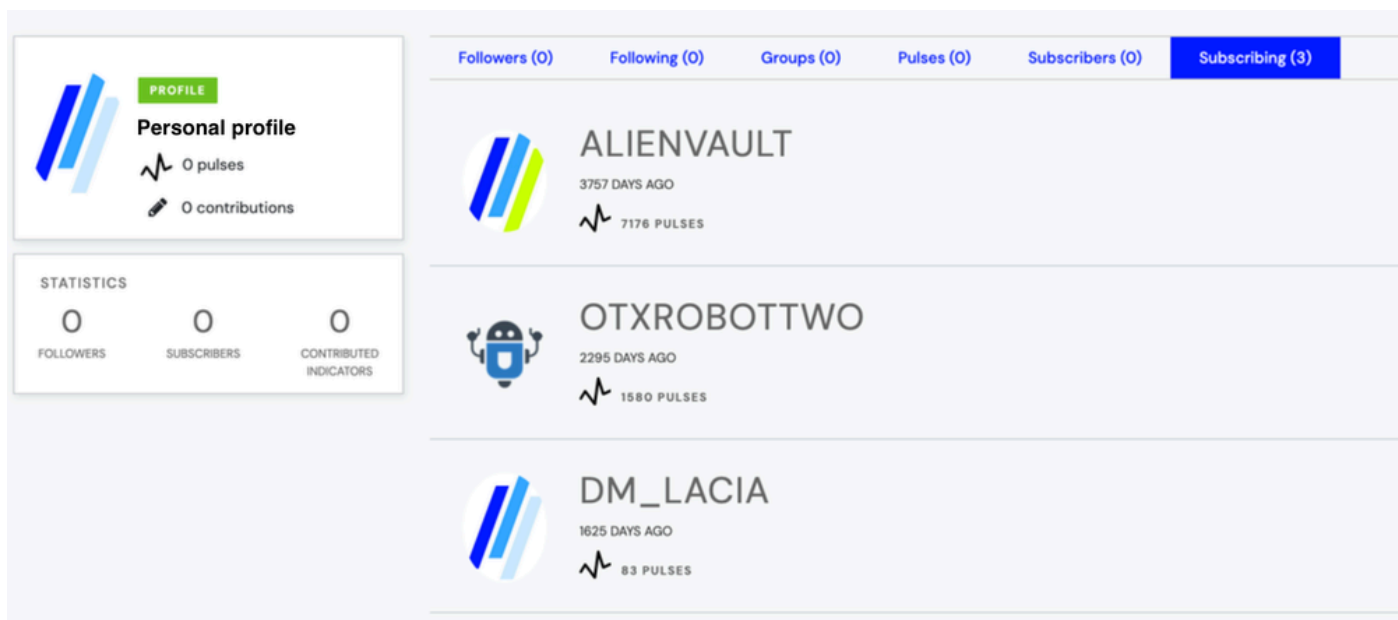
図に示すように、プロセスは情報の取得を開始します。



注：ユーザ名とパスワードを確認するには、次のリンクをチェックしてください。
<https://otx.alienvault.com/api>

AlienVaultプロファイルコレクションサブスクリプション

テストとして、このユーザは3つのプロファイルにサブスクライブしました。



個人プロフィールサブスクリプション

これらのサブスクリプションを取得するには、taxii-collectionsコマンドを使用します。

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

```
(cabby) bash-3.2$ taxii-collections --path https://otx.alienvault.com/taxii/collections --username XXXXXXXXXX --password XXXXXXXXXX
ord anything
2025-05-28 09:57:45.751 INFO: Sending Collection_Information_Request to https://otx.alienvault.com/taxii/collections
=== Data Collection Information ===
Collection Name: user_AlienVault
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: AlienVault
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_diegoher
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: diegoher
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_dm_lacia
Collection Type: DATA_FEED
Available: True
Collection Description: Data feed for user: dm_lacia
Supported Content: All
=== Polling Service Instance ===
Poll Protocol: urn:taxii.mitre.org:protocol:https:1.0
Poll Address: https://otx.alienvault.com/taxii/poll
Message Binding: urn:taxii.mitre.org:message:xml:1.1
=====
=== Data Collection Information ===
Collection Name: user_otxrobbottwo
Collection Type: DATA_FEED
Available: True
```

個人プロフィールコレクション

コレクション名が購読しているコレクション名と同じ場合は、taxii-collectionsコマンドが機能し

ていることを確認できます。

ESAへの送信元の追加

フィードなしのソースの追加

1. Mail Policies > External Threat Feeds Managerの順に移動します。
2. クラスタモードに変更します。
3. Add Sourceをクリックします。
4. ホスト名 : otx.alienvault.com
5. ポーリングパス : /taxi/poll
6. コレクション名 : user_<your_AlienVault_username>
7. ポート : 443
8. ユーザクレデンシャルを設定する : AlienVaultから提供されたクレデンシャルです。
9. Submit > Commit Changesの順にクリックします。

Edit Source

Mode —Cluster: Hosted_Cluster Change Mode...

▶ Centralized Management Options

The settings below are for the configuration of **STIX over TAXII** sources only.

Source Details	
Source Name:	alienvault_diegoher
Description (Optional):	
TAXII Details	
Hostname: ?	otx.alienvault.com
Polling Path: ?	/taxii/poll
Collection Name: ?	user_diegoher
Polling interval:	1 Hours 0 mins (Maximum 24 Hours.)
Age of Threat Feeds: ?	30 Days (Maximum 365 Days.)
Time Span of Poll Segment ?	30 Days The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.
Use HTTPS:	☒ Yes ☐ No Polling Port: ? 443
Configure User Credentials:	☒ Yes ☐ No ☒ Basic Authentication Username: xyz Password:
Proxy Details	
Use Global Proxy:	☐ Yes ☒ No To configure Proxy Server, go to: Security Services > Security Updates

Cancel Submit

パーソナルソース

フィードなしのポーリングソース

External Threat Feeds Managerでは、送信元が追加されると、新しく追加された送信元が表示されます。

External Threat Feeds Manager

Mode —Cluster: Hosted_Cluster

Change Mode...

▶ Centralized Management Options

External Threat Feed Sources

Add Source

alienvault_diegoher	Hostname otx.alienvault.com Collection Name user_diegoher	1h	10 Jun 2025 12:43:56	Idle	  	Poll Now
---------------------	---	----	----------------------	------	---	----------

* You can configure up to 8 external threat feed sources only.

Key: Polling Suspended

パーソナルフィード

追加したら、Poll Nowをクリックします。

確認

CLIを使用してESAにログインし、脅威フィードログを確認して情報を確認します。

```
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パーソナルポーリング

図に示すように、0個の観測可能なデータがフェッチされたことがわかります。これは、表示されているプロファイルにはフィードが存在しないためです。

フィードを使用したソースの追加

1. Mail Policies > External Threat Feeds Managerの順に移動します。
2. クラスタモードに変更します。
3. Add Sourceをクリックします。
4. ホスト名 : otx.alienvault.com
5. ポーリングパス : /taxi/poll
6. コレクション名 : user_AlienVault
7. ポート : 443
8. ユーザクレデンシャルを設定する : AlienVaultから提供されたクレデンシャルです。
9. Submit > Commit Changesの順にクリックします。

Edit Source

Mode —Cluster: Hosted_Cluster

Change Mode...

Centralized Management Options

The settings below are for the configuration of **STIX over TAXII** sources only.

Source Details

Source Name:

alienvault_diegoher

Description (Optional):

TAXII Details

Hostname: ?

otx.alienvault.com

Polling Path: ?

/taxii/poll

Collection Name: ?

user_AlienVault

Polling interval:

1

Hours

0

mins

(Maximum 24 Hours.)

Age of Threat Feeds: ?

30

Days

(Maximum 365 Days.)

Time Span of Poll Segment ?

30

Days

The maximum time span for a poll segment is the value entered in the 'Age of Threat Feeds' field.

Use HTTPS:

☒ Yes ☐ No

Polling Port: ?

443

Configure User Credentials:

☒ Yes ☐ No

☒ Basic Authentication

Username:

xyz

Password:

.....

Proxy Details

Use Global Proxy:

☐ Yes ☒ No

To configure Proxy Server, go to: [Security Services > Security Updates](#)

CancelSubmit

Alienvaultソース

フィードを使用したソースのポーリング

External Threat Feeds Managerでは、送信元が追加されると、新しく追加された送信元が表示されます。

External Threat Feeds Manager

Mode —Cluster: Hosted_Cluster

Change Mode...

▶ Centralized Management Options

External Threat Feed Sources

Add Source

alienvault_diegoher	Hostname otx.alienvault.com Collection Name user_AlienVault	1h	10 Jun 2025 12:43:56	Idle			Poll Now
---------------------	---	----	----------------------	------	-------------	-------------	----------

* You can configure up to 8 external threat feed sources only.

Key:

Polling Suspended

Alienvaultフィード

追加したら、[Poll Now]をクリックします。

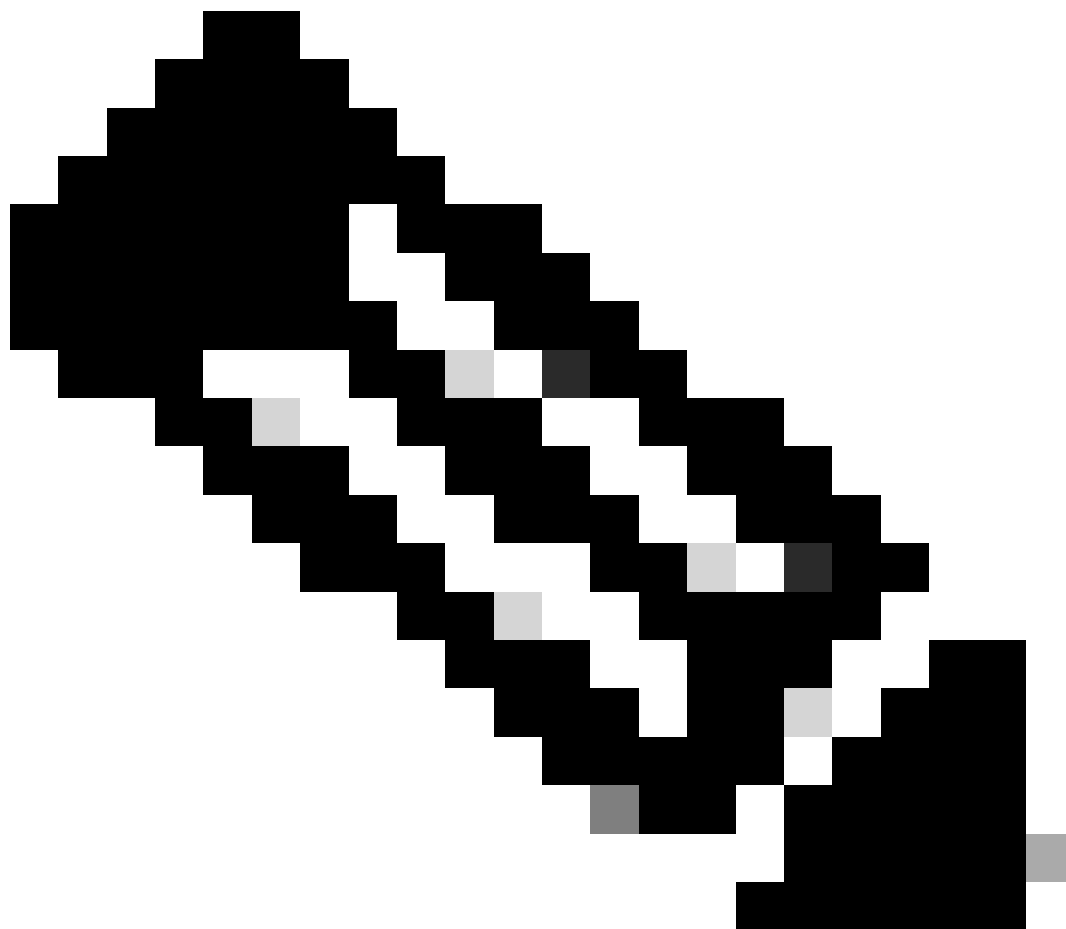
確認

CLIを使用してESAにログインし、脅威フィードログを確認して情報を確認します。

```
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
```

alienvaultフィードのポーリング

図に示すように、いくつかの観測可能なデータがフェッチされたことがわかります。



注：新しいフィードが設定済みのコレクションに追加されると、ESAが自動的に送信元
をポーリングし、新しい観測可能データが取得されます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。