



Conectar TAXII Feed's externos

.....

Guía para conectar TAXII Feeds de fuentes de terceros, gratuitas o pagas, cloud u onprem.

EDSI Trend Argentina.



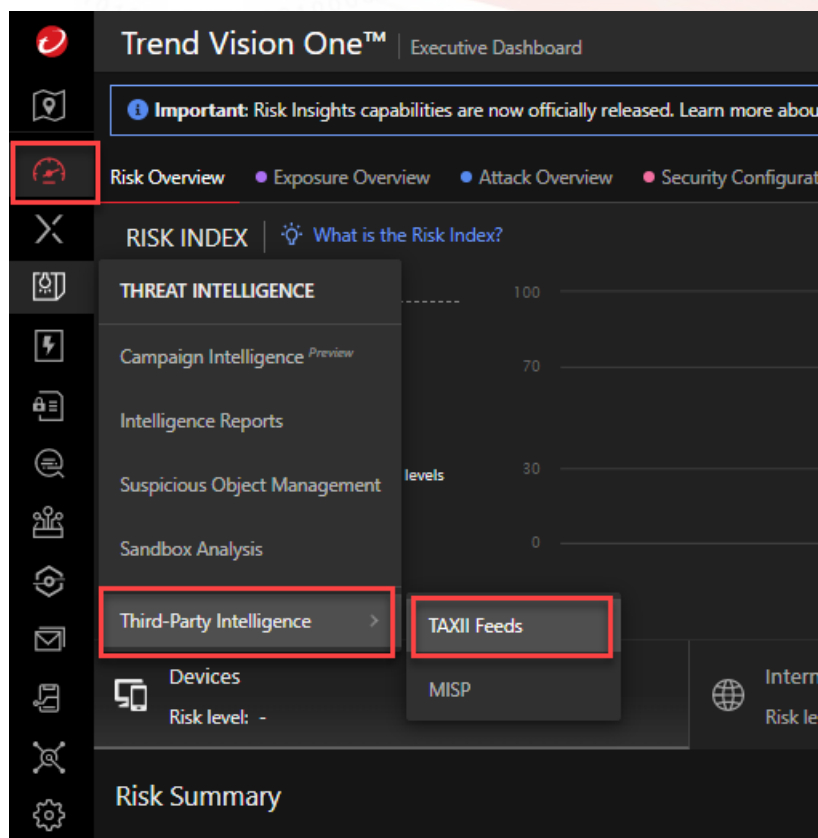
EDSI Trend

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 - 6000
www.trendargentina.com.ar

Página 1

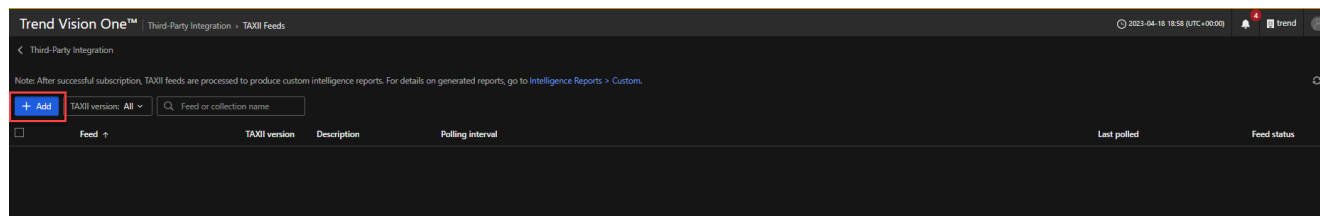
Desde V1 nos dirigimos a:

THREAT INTELLIGENCE → THIRD PARTY INTEGRATION → TAXII FEEDS



En la siguiente pestaña, se nos desplegará los distintos TAXII Feeds que tengamos configurados.

Si no tenemos ninguno, simplemente clickearemos en el apartado **"ADD"**.



En el siguiente apartado, vamos a encontrar distintas configuraciones que deberemos tomar de nuestro servidor de TAXII Feed o, en su defecto, de algún TAXII Feed cloud.

Trend Vision One™ | Third-Party Integration > TAXII Feeds > Add

Enable access to the following FQDN/IP addresses for your deployment region in your TAXII server:

Public IP	FQDN
3.228.232.225	tpi-external-us.xdr.trendmicro.com

General

Status: ☒ Enabled

TAXII version:

Discovery URL*:

Description:

☐ Use CA certificate

☐ Specify authentication credentials

☐ Server requires client authentication

Collections

Collection
No data to display Click to explore available collections.

Polling criteria

Polling interval*: at :

Poll information for*:

 **EDSI Trend**

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 - 6000
www.trendargentina.com.ar

Página 3

NOTA: Recordar que si queremos configurar un TAXII Feed Onprem, debemos garantizar que el mismo logre tener acceso a URL's de Trend Micro.

Enable access to the following FQDN/IP addresses for your deployment region in your TAXII server:

Public IP	FQDN
3.228.232.225	tpi-external-us.xdr.trendmicro.com

Como ejemplo, tomamos el TAXII Feed gratuito de Alienvault, el cual dispone versión 2.1.

Fuente: <https://otx.alienvault.com/api>

DirectConnect API

The OTX DirectConnect API allows you to easily synchronize the Threat Intelligence available in OTX to the tools you use to monitor your environment. Using the DirectConnect agents you can integrate with your infrastructure to detect threats targeting your environment. If there is no pre-built agent for the products you are using, leverage the DirectConnect SDK (available in Java and Python) to develop your own integration for the community.

Resources

Docs

TAXII

Example API Uses

OTX can act as a TAXII server, making it possible for you to consume pulses via any TAXII client that you prefer.

Getting set up

To consume the OTX STIX/TAXII feed you'll need to enter the following details into your TAXII client:

Discovery URL: <https://otx.alienvault.com/taxii/discovery>

Username: (Your API key)

Password: (put anything here, password is ignored)

How are you using STIX/TAXII?

Despite a mammoth specification, we found there is little standardisation in the way TAXII client implementations work. For example, some clients will poll for updates every minute, some every hour. Some clients do not properly do "paging" of results. Let us know if our implementation isn't working for your client, or if you have any questions or suggestions.

DirectConnect API Usage

Your OTX Key:

Using API: ✕

Connect to AlienVault USM™ or AlienVault OSSIM™

Already using AlienVault USM or AlienVault OSSIM? If so, use your OTX API key with USM / OSSIM and get the benefits of the DirectConnect API immediately.

Don't have AlienVault USM? Try AlienVault USM.

Allí, encontraremos el paso a paso para poder conectar el TAXII Feed gratuito a la consola de V1.

Nos indica paso a paso:

1. Crear una cuenta en Alienvault.
2. Definir la versión de TAXII en 2.1
3. Utilizar el Discovery URL (El portal de alienvault trae la url 1.0, la URL correcta la detallaremos a continuación).
4. Utilizar el API Key generado con la cuenta de Alienvault como Username en V1.
5. Utilizar un * como password para autenticar en V1.



EDSI Trend

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 – 6000
www.trendargentina.com.ar

Página 4

Trend Vision One™ | Third-Party Integration > TAXII Feeds > Add

General

Status: ☒ Enabled

TAXII version:

Discovery URL:*

Description:

☐ Use CA certificate

☒ Specify authentication credentials

User name:*

Password:*

☐ Server requires client authentication

Collections

Collection

Una vez cargado los campos, si hacemos click en Discover podemos identificar cuales son los indicadores de compromiso que se traerán a la consola de V1.

Collections

Collection

Open Threat Exchange TAXII Server

	Collection name ^	Extract and block suspicious objects ⓘ	Run an auto sweep ⓘ
<input type="checkbox"/>	Your pulse subscription	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Data feed for user: AlienVault	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Data feed for user: Mauricio14092001	<input type="checkbox"/>	<input type="checkbox"/>



EDSI Trend

Avda. Corrientes 1386 Piso 8
CP- 1043ABN - Capital Federal – República Argentina
Teléfono: 0810 – 362 - 6000
www.trendargentina.com.ar

Página 5

Discover Selected collections: 1

Collection	Collection name ↑	Extract and block suspicious objects ⓘ	Run an auto sweep ⓘ
Open Threat Exchange TAXII Server			
<input type="checkbox"/>	Your pulse subscription	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Data feed for user: AlienVault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Data feed for user: Mauricio14092001	<input type="checkbox"/>	<input type="checkbox"/>

Seleccionado la cadena de IOC's que vamos a querer traer a V1, podemos modificar el tipo de indicador que queremos que se cargue;

<input type="checkbox"/>	Your pulse subscription	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Data feed for user: AlienVault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Data feed for user: Mauricio14092001	<input type="checkbox"/>	<input type="checkbox"/>

Object Type Settings

Select the types of objects to extract and add to the Suspicious Object List as high-risk objects with Block/Quarantine action applied.

- ☒ Domain
- ☒ Sender address
- ☒ IP address
- ☒ File SHA-1
- ☒ File SHA-256
- ☒ URL

Finalmente, resta configurar en qué momentos o en qué horario se realizará la búsqueda de IOC's y cuando se cargaran a V1.

Polling criteria

Polling interval:* at :

Poll information for:*



Para validar que efectivamente se estén cargando los IOC's, podemos corroborarlo en el apartado de Suspicious Object List;

Suspicious Object List										Applicable products: 5
<div> <div>+ Add</div> <div>Last updated: All</div> <div>Object type: All</div> <div>Source: All</div> <div>Q Object, Source...</div> </div>										
Object	Risk level	Action	Expiration	Source	Source details	Description	Last updated			
4D92A4CEB20237647A202CD9D94D5A29C1A14B274D729E9C8C...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 09:15:59			
8926FCD53FF8361439CDA7EAA4F69330A38971D	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
4C848E586A891694A0F81350CFE8379FCAD692872A383671CE420...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
5F4713D82DC112828D93FE54E7FE622A888A	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
79C0C48614379371E3DA809C512A945C19F48B326D2D28EA1603F83...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
44A1146173D80663A237878F88120F39558C33E60E73ECC798953E...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
84349F2EFF8DD651458C831D38155346C1E2D308191BF37197FFA51...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
57E4C16750F2AD1DE1E22A5D0749A8DC4FEDF88132C0AD6C83506...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
0C0C38968887754634EFD42143F78D16377A8577A87AC839C7E...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
490F03BCD7720254C5231A9A20748656E78863AFDDC3EEA71EDACD...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
loop2.hugonet	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
1CBA58F73221858879308FEA80106AE5415E70F49A59572702DC9F...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
001E866FAAFC8CA823F5E490F3080F985C83D382A455F9C9C39...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
AE43978526E6624379D675E1CA6D079F1C3D236D81711C7D1835...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
1889CA9313C9F14FCF3AD6D1EF731FF83D227FA3439D457EAC90F...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			
F6AB4045CA29BA398BDCB278D6E63FC971D138F88F03AEAD213D...	High	Block / Quarantine	2023-06-17 06:15:40	Third-party intelligen...	obt.alienvault.com - Data feed for ...	Data feed for user: AlienVault	2023-04-18 06:15:48			

