



UNIVERSIDADE  
LUSÓFONA

# Trabalho Final De Curso

Guia de Configuração de Conectores do OpenCTI

**Miguel Lourenço**

**Vasco Pereira**

12/1/2025

[www.ulusofona.pt](http://www.ulusofona.pt)

# Índice

Índice .....	ii
Lista de Figuras .....	iii
Resumo.....	4
Configuração do Ficheiro Compose .....	5
AbuseIPDB.....	6
MalwareBazaar .....	8
AlienVault OTX .....	10
Virustotal.....	12
Phishunt .....	14
URLhaus.....	16
Conector Misp ao OpenCTi .....	18
Compilação e Verificação no OpenCTI .....	22
Bibliografia .....	25

## Lista de Figuras

Figura 1	5
Figura 2	6
Figura 3	7
<i>Figura 4</i>	7
Figura 5	8
Figura 6	9
Figura 7	10
Figura 8	11
Figura 9	11
Figura 10	12
Figura 11	13
Figura 12	14
Figura 13	15
Figura 14	16
Figura 15	17
Figura 16	18
Figura 17	20
Figura 18	20
Figura 19	21
Figura 20	22
Figura 21	23
Figura 22	23
Figura 23	24
Figura 24	24

## Resumo

O objetivo desta tarefa é proceder à integração das fontes públicas na plataforma OpenCTI, permitindo que os dados dessas fontes sejam visualizados e analisados diretamente na plataforma.

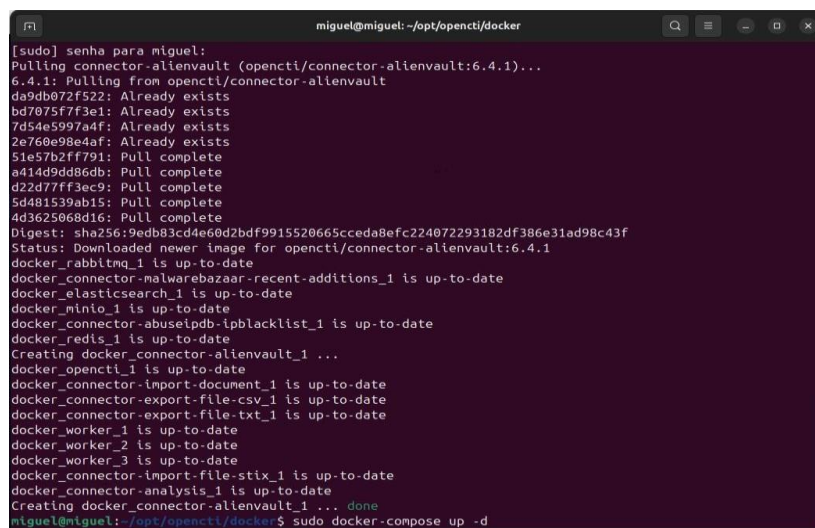
A configuração pode ser feita seguindo as instruções do guia oficial da [OpenCTI], garantindo o acesso eficiente às informações para consulta e análise.

## Configuração do Ficheiro Compose

A configuração dos conectores é feita no ficheiro `docker-compose.yml`. O primeiro passo é abrir o ficheiro, sendo que, para facilitar a edição, deve-se usar o Sublime Text com o seguinte comando: **`sudo subl docker-compose.yml`**.

**Figura 1**

*Configuração inicial do Docker-compose.yml*



```
miguel@miguel: ~/opt/opencti/docker
[sudo] senha para miguel:
Pulling connector-alienvault (opencti/connector-alienvault:6.4.1)...
6.4.1: Pulling from opencti/connector-alienvault
da9db072f522: Already exists
bd7075f7f3e1: Already exists
7d54e597a4f: Already exists
2e760e98e4af: Already exists
51e57b2ff791: Pull complete
a414d9dd86db: Pull complete
d22d77ff3ec9: Pull complete
5d481539ab15: Pull complete
4d3625068d16: Pull complete
Digest: sha256:9edb83cd4e60d2bdf9915520665cceda8efc224072293182df386e31ad98c43f
Status: Downloaded newer image for opencti/connector-alienvault:6.4.1
docker_rabbitmq_1 is up-to-date
docker_connector-malwarebazaar-recent-additions_1 is up-to-date
docker_elasticsearch_1 is up-to-date
docker_minio_1 is up-to-date
docker_connector-abuseipdb-ipblacklist_1 is up-to-date
docker_redis_1 is up-to-date
Creating docker_connector-alienvault_1 ...
docker_opencti_1 is up-to-date
docker_connector-import-document_1 is up-to-date
docker_connector-export-file-csv_1 is up-to-date
docker_connector-export-file-txt_1 is up-to-date
docker_worker_1 is up-to-date
docker_worker_2 is up-to-date
docker_worker_3 is up-to-date
docker_connector-import-file-stix_1 is up-to-date
docker_connector-analysis_1 is up-to-date
Creating docker_connector-alienvault_1 ... done
miguel@miguel:~/opt/opencti/docker$ sudo docker-compose up -d
```

Após abrir o ficheiro, devemos começar a adicionar os conectores necessários para o sucesso deste projeto. Para isso, é necessário aceder ao seguinte endereço: <https://github.com/OpenCTIPlatform/connectors/tree/master/external-import>, onde se encontram diversos conectores oficiais para o OpenCTI.

# AbuseIPDB

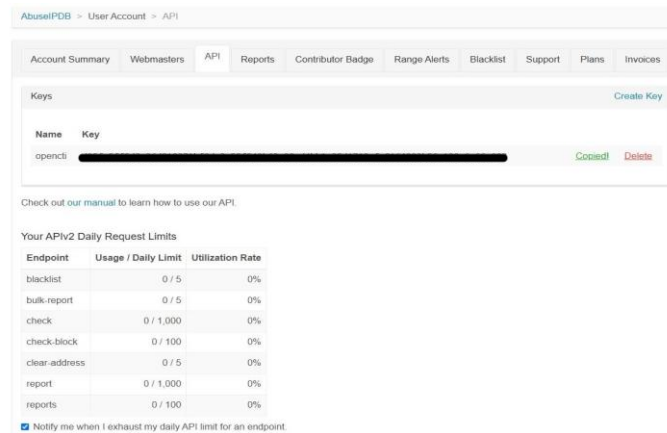
Este conector está disponível em <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/abuseipdb-ipblacklist>, onde devemos aceder à pasta **Docker-compose.yml**. Dentro desta pasta, encontramos as configurações necessárias para adicionar ao nosso ficheiro **docker-compose.yml** original.

**Figura 2**

*Conector do abuseIP*

```
1  version: '3'
2  services:
3    connector-abuseipdb-ipblacklist:
4      image: opencti/connector-abuseipdb-ipblacklist:6.4.2
5      environment:
6        - OPENCTI_URL=http://opencti:8080
7        - OPENCTI_TOKEN=ChangeMe
8        - CONNECTOR_ID=ChangeMe # Valid UUIDv4
9        - "CONNECTOR_NAME=AbuseIPDB IP Blacklist"
10       - CONNECTOR_SCOPE=abuseipdb
11       - CONNECTOR_LOG_LEVEL=error
12       - ABUSEIPDB_URL=https://api.abuseipdb.com/api/v2/blacklist
13       - ABUSEIPDB_API_KEY=ChangeMe
14       - ABUSEIPDB_SCORE=100
15       - ABUSEIPDB_LIMIT=10000
16       - ABUSEIPDB_INTERVAL=2 #Day
17     restart: always
```

Para utilizar este conector, é necessário criar uma conta no site <https://www.abuseipdb.com/account/api> para obter uma chave de API autenticada, que será essencial para a configuração correta do conector.

**Figura 3***Api key do AbuseIP*

Após obter a chave de API, é necessário alterar todos os campos com “ChangeMe” para garantir que a configuração está correta. Estes campos devem ser substituídos com as informações apropriadas, conforme o exemplo abaixo.

Além disso, para os campos que contêm o **CONNECTOR\_ID**, pode-se gerar um ID único através do site [uuidv4], que fornecerá o UUID necessário para completar a configuração.

**Figura 4***Conector do abuseIP dentro do documento do Docker-compose*

```
connector-abuseipdb-ipblacklist:
  image: openciti/connector-abuseipdb-ipblacklist:6.4.1
  environment:
    - OPENCITI_URL=http://openciti:8080
    - OPENCITI_TOKEN=${OPENCITI_ADMIN_TOKEN}
    - CONNECTOR_ID=a982239c-7786-46b4-96b8-2a7115b56882
    - "CONNECTOR_NAME=AbuseIPDB IP Blacklist"
    - CONNECTOR_SCOPE=abuseipdb
    - CONNECTOR_LOG_LEVEL=error
    - ABUSEIPDB_URL=https://api.abuseipdb.com/api/v2/blacklist
    - ABUSEIPDB_API_KEY=ChangeMe
    - ABUSEIPDB_SCORE=100
    - ABUSEIPDB_LIMIT=10000
    - ABUSEIPDB_INTERVAL=2 #Day
  restart: always
```

# MalwareBazaar

Este conector está disponível em <https://github.com/OpenCTIPlatform/connectors/tree/master/external-import/malwarebazaar-recentadditions>, onde devemos aceder à pasta **Docker-compose.yml**. Dentro desta pasta, encontraremos as configurações necessárias para adicionar ao nosso ficheiro **docker-compose.yml** original.

**Figura 5**

*Conector do abuse*

```
1  version: '3'
2  services:
3    connector-malwarebazaar-recent-additions:
4      image: opentcti/connector-malwarebazaar-recent-additions:6.4.2
5      environment:
6        - OPENTCTI_URL=http://opentcti:8080
7        - OPENTCTI_TOKEN=ChangeMe
8        - CONNECTOR_ID=ChangeMe
9        - "CONNECTOR_NAME=MalwareBazaar Recent Additions"
10       - CONNECTOR_LOG_LEVEL=error
11       - MALWAREBAZAAR_RECENT_ADDITIONS_API_URL=https://mb-api.abuse.ch/api/v1/
12       - MALWAREBAZAAR_RECENT_ADDITIONS_COOLDOWN_SECONDS=300 # Time to wait in seconds between subsequent requests
13       - MALWAREBAZAAR_RECENT_ADDITIONS_INCLUDE_TAGS=exe,dll,docm,docx,doc,xls,xlsx,xls#,js # (Optional) Only download files if any tag
14       - MALWAREBAZAAR_RECENT_ADDITIONS_INCLUDE_REPORTERS= # (Optional) Only download files uploaded by these reporters. (comma separate
15       - MALWAREBAZAAR_RECENT_ADDITIONS_LABELS=malware-bazaar # (Optional) Labels to apply to uploaded Artifacts. (comma separated)
16       - MALWAREBAZAAR_RECENT_ADDITIONS_LABELS_COLOR=#54483b # color to use for labels
17      restart: always
```

Após aceder à pasta e obter os ficheiros necessários, é preciso alterar todos os campos com "ChangeMe" para garantir que a configuração esteja correta. Estes campos devem ser substituídos com as informações adequadas, conforme o exemplo abaixo.

Além disso, para os campos que contêm **CONNECTOR\_ID**, deverá gerar um ID único utilizando o [uuidv4] Esse UUID gerado será usado para preencher corretamente o campo **CONNECTOR\_ID** na configuração.



Figura 6

Conector do MalwareBazaar dentro do documento do Docker-compose

```
connector-malwarebazaar-recent-additions:
  image: opentti/connector-malwarebazaar-recent-additions:6.4.1
  environment:
    - OPENTTI_URL=http://opentti:8080
    - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
    - CONNECTOR_ID=ee81146-0860-44f1-93c3-b911e55ec9b2
    - "CONNECTOR_NAME=MalwareBazaar Recent Additions"
    - CONNECTOR_LOG_LEVEL=error
    - MALWAREBAZAAR_RECENT_ADDITIONS_API_URL=https://mb-api.abuse.ch/api/v1/
    - MALWAREBAZAAR_RECENT_ADDITIONS_COOLDOWN_SECONDS=300 # Time to wait in seconds between subsequent requests
    - MALWAREBAZAAR_RECENT_ADDITIONS_INCLUDE_TAGS=exe,dll,docm,docx,doc,xls,xlsx,xlsm,js # (Optional) Only download files if any tag matches. (Comma separated)
    - MALWAREBAZAAR_RECENT_ADDITIONS_INCLUDE_REPORTERS= # (Optional) Only download files uploaded by these reporters. (Comma separated)
    - MALWAREBAZAAR_RECENT_ADDITIONS_LABELS=malware-bazaar # (Optional) Labels to apply to uploaded Artifacts. (Comma separated)
    - MALWAREBAZAAR_RECENT_ADDITIONS_LABELS_COLOR=#54483b # Color to use for labels
  restart: always
```

# AlienVault OTX

Este conector está disponível em <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/alienvault>, onde devemos aceder à pasta **Docker-compose.yml**. Dentro dessa pasta, encontrará as configurações necessárias para adicionar ao nosso **docker-compose.yml** original.

**Figura 7**  
*Conector AlienOTX*

```
1 version: '3'
2 services:
3   connector-alienvault:
4     image: opencti/connector-alienvault:6.4.2
5     environment:
6       - OPENCTI_URL=https://opencti:8080
7       - OPENCTI_TOKEN=ChangeMe
8       - CONNECTOR_ID=ChangeMe
9       - CONNECTOR_NAME=alienvault
10      - CONNECTOR_SCOPE=alienvault
11      - CONNECTOR_LOG_LEVEL=error
12      - CONNECTOR_DURATION_PERIOD=PT30M # In ISO8601 format starting with "P" for Period ex: "PT30M" = Period time of 30 minutes
13      - ALIENVAULT_SQS_URL=https://otx.alienvault.com
14      - ALIENVAULT_API_KEY=ChangeMe
15      - ALIENVAULT_TLP=White
16      - ALIENVAULT_CREATE_OBSERVABLES=true
17      - ALIENVAULT_CREATE_INDICATORS=true
18      - ALIENVAULT_PULSE_START_TIMESTAMP=2022-05-01T00:00:00 # REMARK! Could be a lot of pulses!
19      - ALIENVAULT_REPORT_TYPE=threat-report
20      - ALIENVAULT_REPORT_STATUS=New
21      - ALIENVAULT_GUESS_MALWARE=false # Use Tags to guess malware.
22      - ALIENVAULT_GUESS_CVE=false # Use Tags to guess CVE.
23      - ALIENVAULT_EXCLUDED_PULSE_INDICATOR_TYPES=Fileman-PDS,Fileman-SMS # Excluded Pulse Indicator types.
24      - ALIENVAULT_ENABLE_RELATIONSHIPS=true # Enable/Disable relationship creation between SDOs.
25      - ALIENVAULT_ENABLE_ATTACK_PATTERNS_INDICATES=false # Enable/Disable "Indicates" relationships between indicators and attack patterns
26      - ALIENVAULT_INTERVAL_SEC=1800
27      - ALIENVAULT_IMPORT_X_OPENCTI_SCORE=50
28      - ALIENVAULT_X_OPENCTI_SCORE_IMPORT=0
29      - ALIENVAULT_X_OPENCTI_SCORE_DOMAIN=70
30      - ALIENVAULT_X_OPENCTI_SCORE_HOSTNAME=75
31      - ALIENVAULT_X_OPENCTI_SCORE_IPv4=70
32      - ALIENVAULT_X_OPENCTI_SCORE_IPv6=45
33      - ALIENVAULT_X_OPENCTI_SCORE_URL=80
34      - ALIENVAULT_X_OPENCTI_SCORE_RUTEX=40
35      - ALIENVAULT_X_OPENCTI_SCORE_CRYPTOCURRENCY_WALLET=80
36      restart: always
```

Para utilizar este conector, é necessário criar uma conta no site <https://otx.alienvault.com/settings> para obter uma chave de API autenticada, que será essencial para a configuração correta do conector.



# Virustotal

Este conector está disponível em: <https://github.com/OpenCTIPlatform/connectors/tree/master/externalimport/virustotal-livehunt-notifications>, onde devemos acessar à pasta **Docker-compose.yml**. Lá encontraremos as configurações necessárias para integrar este conector ao nosso ficheiro **docker-compose.yml** original.

**Figura 10**

*Conector do Virustotal*

```
1  version: '3'
2  services:
3    connector-virustotal-livehunt-notifications:
4      image: opentti/connector-virustotal-livehunt-notifications:6.4.2
5      environment:
6        - OPENCTI_URL=http://opentti:8080
7        - OPENCTI_TOKEN=ChangeMe
8        - CONNECTOR_ID=Virustotal_Livehunt_Notifications
9        - "CONNECTOR_NAME=VirusTotal Livehunt Notifications"
10       - CONNECTOR_SCOPE=StixFile,Indicator,Incident
11       - CONNECTOR_LOG_LEVEL=error
12       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_API_KEY=ChangeMe # Private API Key
13       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_INTERVAL_SEC=300 # Time to wait in seconds between subsequent requests
14       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_ALERT=True # Set to true to create alerts
15       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_EXTENSIONS='exe,dll' # (Optional) Comma separated filter to only download files matching these extensions
16       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MIN_FILE_SIZE=1000 # (Optional) Don't download files smaller than this many bytes
17       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MAX_FILE_SIZE=52428800 # (Optional) Don't download files larger than this many bytes
18       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MAX_AGE_DAYS=3 # Only create the alert if the first submission of the file is not older than 'max_age_days'
19       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_MIN_POSITIVES=5 # (Optional) Don't download files with less than this many vendors marking malicious
20       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_FILE=True # Set to true to create file object linked to the alerts
21       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_UPLOAD_ARTIFACT=False # Set to true to upload the file to opentti
22       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_CREATE_YARA_RULE=True # Set to true to create yara rule linked to the alert and the file
23       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_DELETE_NOTIFICATION=False # Set to true to remove livehunt notifications
24       - VIRUSTOTAL_LIVEHUNT_NOTIFICATIONS_FILTER_WITH_TAG='mytag' # Filter livehunt notifications with this tag
25      restart: always
```

Para utilizar este conector, é necessário criar uma conta no site <https://www.virustotal.com/gui/myapikey> para obter uma chave de API autenticada, que será necessária para a configuração correta do conector.

Após obter a chave de API, é necessário substituir todos os campos com "ChangeMe" na configuração para garantir que tudo esteja corretamente configurado, seguindo o exemplo fornecido.



# Phishunt

Este conector está disponível em <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/phishunt>. Devemos aceder à pasta **Docker-compose.yml**, onde se encontram as configurações necessárias para integrar este conector no ficheiro **docker-compose.yml** original.

**Figura 12**

*Conector do Phishunt*

```
1  version: '3'
2  services:
3    connector-phishunt:
4      image: opencti/connector-phishunt:6.4.2
5      environment:
6        - OPENCTI_URL=http://opencti:8080
7        - OPENCTI_TOKEN=ChangeMe(UUIDv4 token)
8        - CONNECTOR_ID=ChangeMe(UUIDv4 token)
9        - CONNECTOR_NAME=Phishunt
10       - CONNECTOR_SCOPE=phishunt
11       - CONNECTOR_CONFIDENCE_LEVEL=40 # From 0 (Unknown) to 100 (Fully trusted)
12       - CONNECTOR_LOG_LEVEL=error
13       - PHISHUNT_API_KEY= # Optional, if not provided, consume only https://phishunt.io/feed.txt
14       - PHISHUNT_CREATE_INDICATORS=true
15       - PHISHUNT_DEFAULT_X_OPENCTI_SCORE=40 # Optional: default is 40
16       - PHISHUNT_X_OPENCTI_SCORE_DOMAIN=40 # Optional
17       - PHISHUNT_X_OPENCTI_SCORE_IP=40 # Optional
18       - PHISHUNT_X_OPENCTI_SCORE_URL=60 # Optional
19       - PHISHUNT_INTERVAL=3 # In days, must be strictly greater than 1
20      restart: always
```

Após aceder ao ficheiro, é necessário substituir todos os campos com "ChangeMe" pelas informações corretas, assegurando que a configuração fique conforme o exemplo fornecido.

Para os campos que contêm **CONNECTOR\_ID**, deve-se gerar um identificador único (UUID) através do [uuidv4] e utilizá-lo nos campos correspondentes.

**Figura 13**

*Conector do Phishunt dentro do documento do Docker-compose*

```
connector-phishunt:
  image: opentti/connector-phishunt:6.4.2
  environment:
    - OPENTTI_URL=http://opentti:8080
    - OPENTTI_TOKEN=${OPENTTI_ADMIN_TOKEN}
    - CONNECTOR_ID=143255-2207-1d71-4110-5-50257-071
    - CONNECTOR_NAME=Phishunt
    - CONNECTOR_SCOPE=phishunt
    - CONNECTOR_CONFIDENCE_LEVEL=40 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=error
    - PHISHUNT_API_KEY= # Optional, if not provided, consume only https://phishunt.io/feed.txt
    - PHISHUNT_CREATE_INDICATORS=true
    - PHISHUNT_DEFAULT_X_OPENTTI_SCORE=40 # Optional: default is 40
    - PHISHUNT_X_OPENTTI_SCORE_DOMAIN=40 # Optional
    - PHISHUNT_X_OPENTTI_SCORE_IP=40 # Optional
    - PHISHUNT_X_OPENTTI_SCORE_URL=60 # Optional
    - PHISHUNT_INTERVAL=3 # In days, must be strictly greater than 1
  restart: always
```

## URLhaus

Este conector está disponível em <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/urlhaus>. Devemos aceder à pasta **Docker-compose.yml**, onde estão as configurações necessárias para integrar este conector no ficheiro **docker-compose.yml** original.

### Figura 14

*Conector do urlhaus*

```
1  version: '3'
2  services:
3    connector-urlhaus:
4      image: opencti/connector-urlhaus:6.4.2
5      environment:
6        - OPENCTI_URL=http://localhost
7        - OPENCTI_TOKEN=ChangeMe
8        - CONNECTOR_ID=ChangeMe
9        - "CONNECTOR_NAME=Abuse.ch URLhaus"
10       - CONNECTOR_SCOPE=urlhaus
11       - CONNECTOR_CONFIDENCE_LEVEL=40 # From 0 (Unknown) to 100 (Fully trusted)
12       - CONNECTOR_LOG_LEVEL=error
13       - URLHAUS_CSV_URL=https://urlhaus.abuse.ch/downloads/csv_recent/
14       - URLHAUS_DEFAULT_X_OPENCTI_SCORE=80 # Optional: Defaults to 80.
15       - URLHAUS_IMPORT_OFFLINE=true
16       - URLHAUS_THREATS_FROM_LABELS=true
17       - URLHAUS_INTERVAL=3 # In days, must be strictly greater than 1
18     restart: always
```

Após aceder ao ficheiro, é necessário substituir todos os campos com "ChangeMe" pelas informações corretas, assegurando que a configuração fique conforme o exemplo fornecido.

Para os campos que contêm **CONNECTOR\_ID**, deve-se gerar um identificador único (UUID) através do [uuidv4] e utilizá-lo nos campos correspondentes.



**Figura 15**

Conector do urlhaus dentro do documento do Docker-compose

```
connector-urlhaus:
  image: openciti/connector-urlhaus:6.4.2
  environment:
    - OPENCITI_URL=http://openciti:8080
    - OPENCITI_TOKEN=${OPENCITI_ADMIN_TOKEN}
    - CONNECTOR_ID=9cdfbefd-b93e-43e7-96b7-1325d6902187
    - "CONNECTOR_NAME=Abuse.ch URLhaus"
    - CONNECTOR_SCOPE=urlhaus
    - CONNECTOR_CONFIDENCE_LEVEL=40 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=error
    - URLHAUS_CSV_URL=https://urlhaus.abuse.ch/downloads/csv_recent/
    - URLHAUS_DEFAULT_X_OPENCITI_SCORE=80 # Optional: Defaults to 80.
    - URLHAUS_IMPORT_OFFLINE=true
    - URLHAUS_THREATS_FROM_LABELS=true
    - URLHAUS_INTERVAL=3 # In days, must be strictly greater than 1
  restart: always
```

# Conector Misp ao OpenCTI

Este conector está disponível em <https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/misp>. Devemos aceder à pasta **Docker-compose.yml**, onde estão as configurações necessárias para integrar este conector no ficheiro **docker-compose.yml** original.

**Figura 16**

*Conector do Misp para ligar ao OpenCTI*

```
image: opencti/connector-misp:6.4.4
environment:
  - OPENCTI_URL=http://localhost
  - OPENCTI_TOKEN=ChangeMe
  - CONNECTOR_ID=ChangeMe
  - CONNECTOR_NAME=MISP
  - CONNECTOR_SCOPE=misp
  - CONNECTOR_LOG_LEVEL=error
  - CONNECTOR_EXPOSE_METRICS=false
  - MISP_URL=http://localhost # Required
  - MISP_REFERENCE_URL= # Optional, will be used to create external reference to MISP event (default is "url")
  - MISP_KEY=ChangeMe # Required
  - MISP_SSL_VERIFY=false # Required
  - MISP_DATETIME_ATTRIBUTE=timestamp # Required, filter to be used in query for new MISP events
  - MISP_DATE_FILTER_FIELD=timestamp # Required, field to filter on date
  - MISP_REPORT_DESCRIPTION_ATTRIBUTE_FILTER= # Optional, filter to be used to find the attribute with report descriptor
  - MISP_CREATE_REPORTS=true # Required, create report for MISP event
  - MISP_CREATE_INDICATORS=true # Required, create indicators from attributes
  - MISP_CREATE_OBSERVABLES=true # Required, create observables from attributes
  - MISP_CREATE_OBJECT_OBSERVABLES=true # Required, create text observables for MISP objects
  - MISP_CREATE_TAGS_AS_LABELS=true # Optional, create tags as labels (sanitize MISP tag to OpenCTI labels)
  - MISP_GUESS_THREAT_FROM_TAGS=false # Optional, try to guess threats (threat actor, intrusion set, malware, etc.) from
  - MISP_AUTHOR_FROM_TAGS=false # Optional, map creator:XX=YY (author of event will be YY instead of the author of the ev
  - MISP_MARKINGS_FROM_TAGS=false # Optional, map marking:XX=YY (in addition to TLP, add XX:YY as marking definition, whe
  - MISP_ENFORCE_WARNING_LIST=false # Optional, enforce warning list in MISP queries
  - MISP_REPORT_TYPE=misp-event # Optional, report_class if creating report for event
  - MISP_IMPORT_FROM_DATE=2000-01-01 # Required, import all event from this date
  - MISP_IMPORT_TAGS= # Optional, list of tags used to filter events to import
  - MISP_IMPORT_TAGS_NOT= # Optional, list of tags to not include
  - MISP_IMPORT_CREATOR_ORGS= # Optional, only import events created by those orgs (put the identifiers here)
  - MISP_IMPORT_CREATOR_ORGS_NOT= # Optional, do not import events created by those orgs (put the identifiers here)
  - MISP_IMPORT_OWNER_ORGS= # Optional, only import events owned by those orgs (put the identifiers here)
  - MISP_IMPORT_OWNER_ORGS_NOT= # Optional, do not import events owned by those orgs (put the identifiers here)
  - MISP_IMPORT_KEYWORD= # Optional, search only events based on a keyword
  - MISP_IMPORT_DISTRIBUTION_LEVELS= # Optional, only import events with the given distribution levels (ex: 0,1,2,3)
  - MISP_IMPORT_THREAT_LEVELS= # Optional only import events with the given threat levels (ex: 1,2,3,4)
  - MISP_IMPORT_ONLY_PUBLISHED=false
  - MISP_IMPORT_WITH_ATTACHMENTS=false # Optional, try to import a PDF file from the attachment attribute
  - MISP_IMPORT_TO_IDS_NO_SCORE=40 # Optional, use as a score for the indicator/observable if the attribute to_ids is no
  - MISP_IMPORT_UNSUPPORTED_OBSERVABLES_AS_TEXT=false # Optional, import unsupported observable as x_opencti_text
  - MISP_IMPORT_UNSUPPORTED_OBSERVABLES_AS_TEXT_TRANSPARENT=true # Optional, import unsupported observable as x_opencti_text
```

Após aceder ao ficheiro, é necessário substituir todos os campos com "ChangeMe" pelas informações corretas, garantindo que a configuração fique conforme o exemplo fornecido.

Para os campos que contêm **CONNECTOR\_ID**, deve-se gerar um identificador único (UUID) utilizando a ferramenta [uuidv4] e utilizá-lo nos respetivos campos.

Além disso, é necessário um Auth Key do MISP para permitir o acesso a partir do conector. Este token deve ser obtido no MISP, dentro das configurações do utilizador, e inserido no campo correspondente.

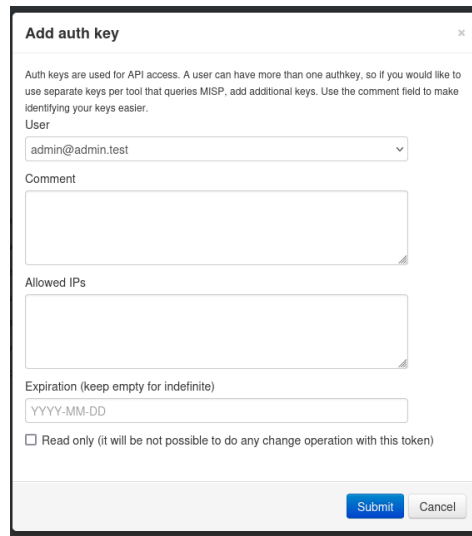
Também é necessário alterar o campo **MISP\_URL** para o URL do MISP da máquina onde este está instalado. Este URL deve refletir o endereço acessível a partir do conector.

Para criar a chave de autenticação no MISP, é necessário seguir os passos abaixo:

1. Aceda ao MISP com um utilizador que possua permissões administrativas.
2. No menu principal, clique na aba **Administration**.
3. Dentro da aba **Administration**, aceda à opção **List Auth Keys**.
4. Nesta secção, é possível criar uma nova chave de autenticação, conforme demonstrado na imagem abaixo.

**Figura 17**

*Configuração de uma chave auth Key no Misp*

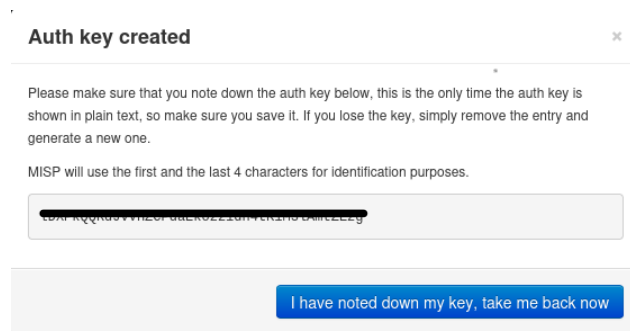


The screenshot shows a web form titled "Add auth key" with a close button (X) in the top right corner. Below the title is a paragraph explaining that auth keys are used for API access and that a user can have more than one. The form contains the following fields and options:

- User:** A dropdown menu with "admin@admin.test" selected.
- Comment:** A large text area.
- Allowed IPs:** A large text area.
- Expiration (keep empty for indefinite):** A text field with the placeholder "YYYY-MM-DD".
- Read only:** A checkbox labeled "Read only (it will be not possible to do any change operation with this token)".
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

**Figura 18**

*Chave Auth key Misp*



The screenshot shows a confirmation message titled "Auth key created" with a close button (X) in the top right corner. The message contains the following text:

Please make sure that you note down the auth key below, this is the only time the auth key is shown in plain text, so make sure you save it. If you lose the key, simply remove the entry and generate a new one.

MISP will use the first and the last 4 characters for identification purposes.

Below the text is a text box containing a long alphanumeric string representing the auth key.

At the bottom right is a blue button labeled "I have noted down my key, take me back now".

Após concluir a criação da chave de autenticação no MISP, pode-se regressar à máquina com o OpenCTI para continuar a configuração do conector. A configuração deve ser ajustada de forma a ficar semelhante à imagem abaixo, com todos os campos devidamente preenchidos, incluindo o **MISP\_URL**, a **Auth Key** gerada, e os demais parâmetros obrigatórios.

Figura 19

Conector do Misp dentro do documento do Docker-compose

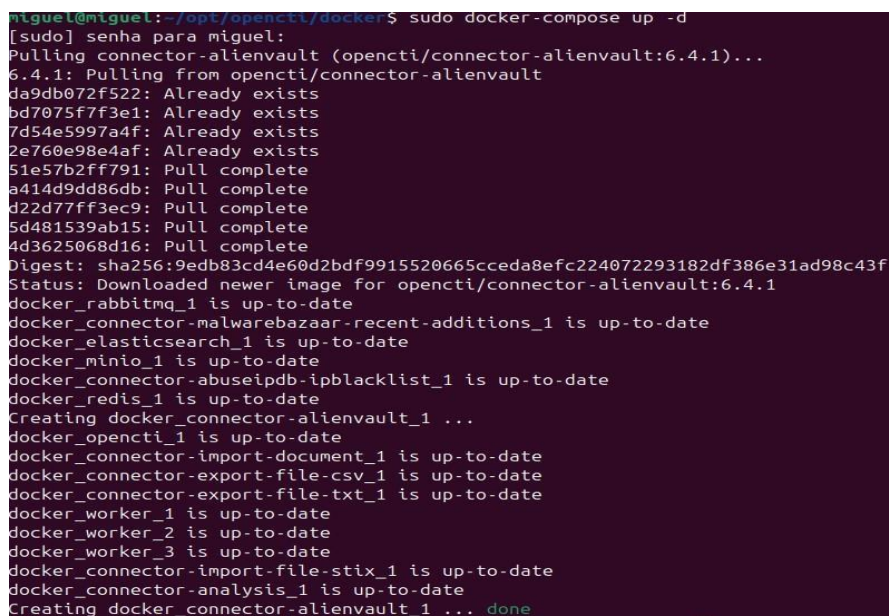
```
image: opencti/opencti:4.10.0
environment:
  - OPENCTI_URL=http://opencti:8080
  - OPENCTI_TOKEN=${OPENCTI_AUTH_TOKEN}
  - CONNECTOR_ID=5ec116f-5b36-4e29-9afc-273df574faf8
  - CONNECTOR_NAME=misp
  - CONNECTOR_SCORE=misp
  - CONNECTOR_LOG_LEVEL=error
  - CONNECTOR_DISABLE_METRICS=false
  - MISP_URL=http://192.168.183.135 # Required
  - MISP_REFERENCE_URL= # Optional, will be used to create external reference to MISP event (default is "url")
  - MISP_REFRESH= # Required
  - MISP_SSL_VERIFY=false # Required
  - MISP_DATE_FILTER_ATTRIBUTE=timestamp # Required, filter to be used in query for new MISP events
  - MISP_DATE_FILTER_FIELD=timestamp # Required, field to filter on date
  - MISP_REPORT_DESCRIPTION_ATTRIBUTE_FILTER= # Optional, filter to be used to find the attribute with report description (example: "type=comment,category=Internal reference")
  - MISP_CREATE_REPORTS=true # Required, create report for MISP event
  - MISP_CREATE_INDICATORS=true # Required, create indicators from attributes
  - MISP_CREATE_OBSERVABLES=true # Required, create observables from attributes
  - MISP_CREATE_OBJECT_OBSERVABLES=true # Required, create text observables for MISP objects
  - MISP_CREATE_TAGS_AS_LABELS=true # Optional, create tags as labels (sanitize MISP tag to OpenCTI labels)
  - MISP_GUESS_THREAT_FROM_TAGS=false # Optional, try to guess threats (threat actor, intrusion set, malware, etc.) from MISP tags when they are present in OpenCTI
  - MISP_AUTHOR_FROM_TAGS=false # Optional, map creator:XXYY (author of event will be YY instead of the author of the event)
  - MISP_MARKINGS_FROM_TAGS=false # Optional, map marking:XXYY (in addition to TLP, add XX:YY as marking definition, where XX is marking type, YY is marking value)
  - MISP_ENFORCE_WARNING_LIST=false # Optional, enforce warning list in MISP queries
  - MISP_REPORT_TYPE=misp-event # Optional, report class if creating report for event
  - MISP_IMPORT_FROM_DATE=2000-01-01 # Required, import all event from this date
  - MISP_IMPORT_TAGS=opencti:import,type:osint,tlp:green # Optional, list of tags used for import events
  - MISP_IMPORT_TAGS_NOT= # Optional, list of tags to not include
  - MISP_IMPORT_CREATOR_ORGS= # Optional, only import events created by those orgs (put the identifiers here)
  - MISP_IMPORT_CREATOR_ORGS_NOT= # Optional, do not import events created by those orgs (put the identifiers here)
  - MISP_IMPORT_OWNER_ORGS= # Optional, only import events owned by those orgs (put the identifiers here)
  - MISP_IMPORT_OWNER_ORGS_NOT= # Optional, do not import events owned by those orgs (put the identifiers here)
  - MISP_IMPORT_KEYWORD= # Optional, search only events based on a keyword
  - MISP_IMPORT_DISTRIBUTION_LEVELS= # Optional, only import events with the given distribution levels (ex: 0,1,2,3)
  - MISP_IMPORT_THREAT_LEVELS= # Optional only import events with the given threat levels (ex: 1,2,3,4)
  - MISP_IMPORT_ONLY_PUBLISHED=false
  - MISP_IMPORT_WITH_ATTACHMENTS=false # Optional, try to import a PDF file from the attachment attribute
  - MISP_IMPORT_TO_ID=NO_SCORECARD # Optional, use as a score for the indicator/observable if the attribute to id is no
  - MISP_IMPORT_UNSUPPORTED_OBSERVABLES_AS_TEXT=false # Optional, import unsupported observable as a opencti text
  - MISP_IMPORT_UNSUPPORTED_OBSERVABLES_AS_TEXT_TRANSPARENT=true # Optional, import unsupported observable as a opencti_text just with the value
  - MISP_INTERVAL= # Required, in minutes
restart: always
```

## Compilação e Verificação no OpenCTI

Após adicionar todas as configurações necessárias ao ficheiro **docker-compose.yml**, deve-se guardar o ficheiro e executar novamente o **docker-compose** para carregar as alterações. Este processo é realizado utilizando o comando `sudo docker-compose up -d`.

**Figura 20**

*Compilação do ficheiro Docker-compose*



```
miguel@miguel:~/opt/opencti/docker$ sudo docker-compose up -d
[sudo] senha para miguel:
Pulling connector-alienvault (opencti/connector-alienvault:6.4.1)...
6.4.1: Pulling from opencti/connector-alienvault
da9db072f522: Already exists
bd7075f7f3e1: Already exists
7d54e5997a4f: Already exists
2e760e98e4af: Already exists
51e57b2ff791: Pull complete
a414d9dd86db: Pull complete
d22d77ff3ec9: Pull complete
5d481539ab15: Pull complete
4d3625068d16: Pull complete
Digest: sha256:9edb83cd4e60d2bdf9915520665cceda8efc224072293182df386e31ad98c43f
Status: Downloaded newer image for opencti/connector-alienvault:6.4.1
docker_rabbitmq_1 is up-to-date
docker_connector-malwarebazaar-recent-additions_1 is up-to-date
docker_elasticsearch_1 is up-to-date
docker_minio_1 is up-to-date
docker_connector-abuseipdb-ipblacklist_1 is up-to-date
docker_redis_1 is up-to-date
Creating docker_connector-alienvault_1 ...
docker_opencti_1 is up-to-date
docker_connector-import-document_1 is up-to-date
docker_connector-export-file-csv_1 is up-to-date
docker_connector-export-file-txt_1 is up-to-date
docker_worker_1 is up-to-date
docker_worker_2 is up-to-date
docker_worker_3 is up-to-date
docker_connector-import-file-stix_1 is up-to-date
docker_connector-analysis_1 is up-to-date
Creating docker_connector-alienvault_1 ... done
```

Após realizar todas as configurações e reiniciar o Docker, abrimos o OpenCTI e verificamos se a integração foi bem-sucedida, conforme ilustrado nas imagens abaixo.

Figura 21

Página inicial do OpenCTI

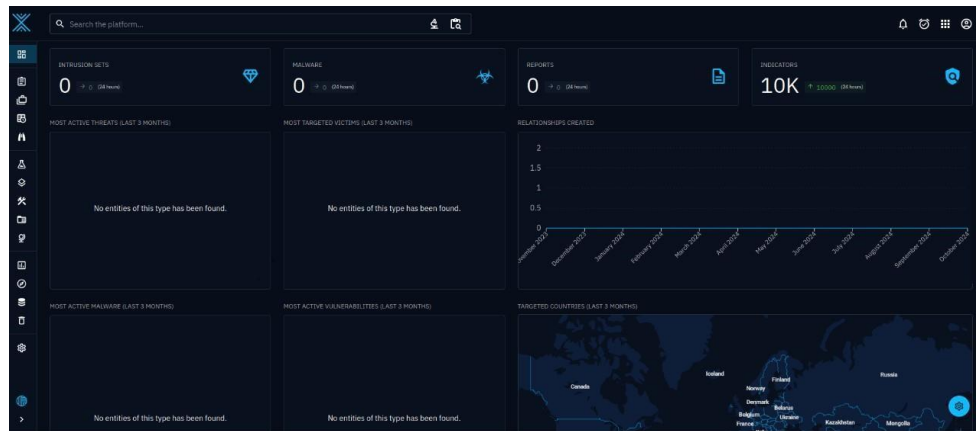


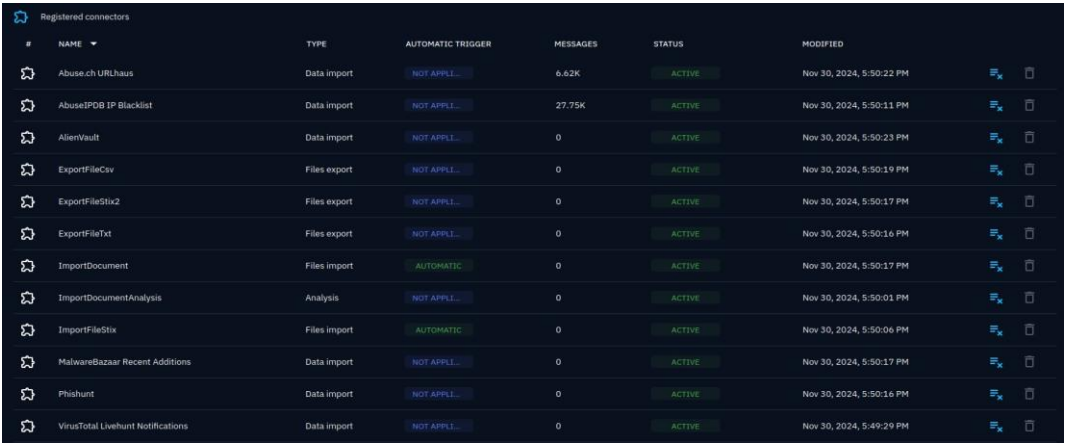
Figura 22

Página de observações do OPenCTI

The screenshot shows the 'Observations / Observables' page in OpenCTI. It features a search bar, a filter dropdown, and a table of results. The table has columns for TYPE, REPRESENTATION, AUTHOR, CREATORS, LABELS, PLATFORM CREATION, and MARKING. The results are filtered by 'Entity type = ARTIFACT'.

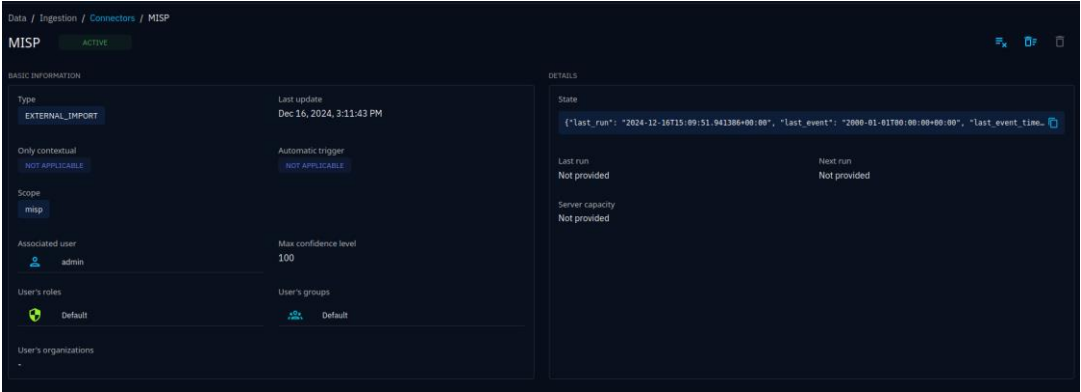
TYPE	REPRESENTATION	AUTHOR	CREATORS	LABELS	PLATFORM CREATION	MARKING
ARTIFACT	307406f0a9a5d3c1548a132fac2313defc0e6b6e60ad832c03...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
ARTIFACT	0049d07099f0c4702ba2d1d40710033020a708f6d3070b6e6a54...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
ARTIFACT	4b414c0d89c2c25d6d9f0e0d070f0e076c2970e9990c17d05172...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
ARTIFACT	a1572376508090c30d069fa7921900fb21177049233b6d4ba7...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
ARTIFACT	c01fa89d072aa10c9345e0440e6a1b0b03197085b230e443c908e...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
ARTIFACT	77aacba2bb6e41672878ba1d1a67ad27e9c530887105d9c26bdc91...	-	admin	Confidential, Restricted	Nov 28, 2024	TOP CLEAR
IPV4 ADDR...	103.78.171.114	AbuseIPDB	admin	No label	Nov 28, 2024	TOP CLEAR
IPV4 ADDR...	220.180.107.193	AbuseIPDB	admin	No label	Nov 28, 2024	TOP CLEAR
IPV4 ADDR...	77.221.138.170	AbuseIPDB	admin	No label	Nov 28, 2024	TOP CLEAR
IPV4 ADDR...	27.254.192.185	AbuseIPDB	admin	No label	Nov 28, 2024	TOP CLEAR
IPV4 ADDR...	104.47.160.162	AbuseIPDB	admin	No label	Nov 28, 2024	TOP CLEAR

**Figura 23**  
*Página dos Conectores OpenCTI*



Registered connectors							
#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	STATUS	MODIFIED	
1	Abuse.ch URLhaus	Data import	NOT APPLICABLE	6.62K	ACTIVE	Nov 30, 2024, 5:50:22 PM	
2	AbuseIPDB IP Blacklist	Data import	NOT APPLICABLE	27.75K	ACTIVE	Nov 30, 2024, 5:50:11 PM	
3	AlienVault	Data import	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:23 PM	
4	ExportFileCsv	Files export	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:19 PM	
5	ExportFileStix2	Files export	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:17 PM	
6	ExportFileTxt	Files export	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:16 PM	
7	ImportDocument	Files import	AUTOMATIC	0	ACTIVE	Nov 30, 2024, 5:50:17 PM	
8	ImportDocumentAnalysis	Analysis	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:01 PM	
9	ImportFileStix	Files import	AUTOMATIC	0	ACTIVE	Nov 30, 2024, 5:50:06 PM	
10	MalwareBazaar Recent Additions	Data import	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:17 PM	
11	Phishhunt	Data import	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:50:16 PM	
12	VirusTotal Livehunt Notifications	Data import	NOT APPLICABLE	0	ACTIVE	Nov 30, 2024, 5:49:29 PM	

**Figura 24**  
*Conector do Misp ao OpenCTI em funcionamento*



Data / Ingestion / Connectors / MISP

**MISP** ACTIVE

**BASIC INFORMATION**

Type: **EXTERNAL\_IMPORT**

Only contextual: **NOT APPLICABLE**

Scope: **misp**

Associated user: **admin**

User's roles: **Default**

User's organizations: **-**

Last update: **Dec 16, 2024, 3:11:43 PM**

Automatic trigger: **NOT APPLICABLE**

Max confidence level: **100**

User's groups: **Default**

**DETAILS**

State: `{"last_run": "2024-12-16T15:09:51.941384+00:00", "last_event": "2000-01-01T00:00:00+00:00", "last_event_time..."}`

Last run: **Not provided**      Next run: **Not provided**

Server capacity: **Not provided**



## Bibliografia

[OpenCTI] Filigran. (2024, June 28). *Installation - OpenCTI Documentation*. Opencti.io.

<https://docs.opencti.io/latest/deployment/installation/#using-docker>

[uuidv4] *Online UUID Generator Tool*. (n.d.). [Www.uuidgenerator.nethttps://www.uuidgenera-](https://www.uuidgenerator.net)

[tor.net/version4](https://www.uuidgenerator.net/version4)

[Sublime Text] Sublime Text. (n.d.). *Sublime Text - A sophisticated text editor for code, markup*

*and prose*. Sublimetext.com. <https://www.sublimetext.com/>