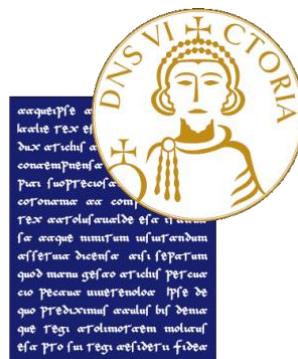


UNIVERSITÀ DEGLI STUDI DEL SANNIO

Dipartimento di Ingegneria
Corso di Laurea Magistrale in Ingegneria Informatica



Progetto di Sicurezza delle Reti e dei Sistemi Software

PIATTAFORMA OPENCTI

Vitaglano Pietro	Mat.: 399000461
Petraccaro Angelo	Mat.: 399000428
Rapuano Antonio	Mat.: 399000429

A.A. 2020/2021

Indice

OPENCTI	5
SCOPO	6
ARCHITETTURA	7
INSTALLAZIONE E CONFIGURAZIONE DI OPENCTI	8
API CLIENTS	15
CLIENT IN PYTHON	15
CLIENT IN Go	15
CONNETTORI OPENCTI	16
DATA IMPORT	16
<i>AlienVault</i>	16
<i>AM!TT</i>	17
<i>CAPE Sandbox</i>	17
<i>CrowdStrike</i>	18
<i>Cryptolaemus</i>	18
<i>Cuckoo Sandbox</i>	19
<i>CVE Database</i>	19
<i>Cyber Threat Coalition (COVID-19)</i>	19
<i>Cybercrime Tracker</i>	20
<i>Files restore</i>	20
<i>FireEye</i>	21
<i>Kaspersky</i>	21
<i>LastInfoSec</i>	22
<i>Malpedia</i>	22
<i>MISP</i>	23
<i>MITRE ATT&CK</i>	23
<i>OpenCTI datasets</i>	24
<i>RiskIQ</i>	24
<i>Sekoia</i>	25
<i>TAXII2</i>	25
<i>TheHive</i>	26
<i>ThreatMatch</i>	27
<i>URLhause by Abuse.ch</i>	27
<i>Valhalla</i>	28

<i>Virustotal Livehunt</i>	28
<i>VX Vault</i>	28
<i>Yeti</i>	28
STREAM CONSUMER.....	29
<i>Backup Files</i>	29
<i>Elastic</i>	29
<i>History</i>	30
<i>QRadar</i>	30
<i>Splunk</i>	30
<i>Tanium</i>	31
<i>Tenzir → ThreatBus</i>	31
INTERNAL ENRICHMENT.....	32
<i>AbuseIPDB</i>	32
<i>CAPE Sandbox</i>	32
<i>Gatewatcher Lastinfosec</i>	33
<i>GreyNoise</i>	33
<i>Hatching Triage Sandbox</i>	34
<i>Hybrid Analysis</i>	34
<i>Hygiene</i>	35
<i>Import External Reference</i>	36
<i>Intezer Sandbox</i>	36
<i>IPinfo</i>	37
<i>Ivre</i>	37
<i>Malbeacon</i>	38
<i>Shodan</i>	38
<i>Unpac-me</i>	39
<i>VirusTotal</i>	39
FILE IMPORT.....	40
<i>ImportFileStix</i>	40
<i>ImportReport (PDF)</i>	41
FILE EXPORT	42
<i>ExportFileCSV</i>	42
<i>ExportFileSTIX</i>	42
<i>ExportFileTXT</i>	42
THIRD PARTY MODULES & PLUG-IN	43
<i>Cortex</i>	43
<i>Maltego</i>	44
CONNETTORI CUSTOM.....	45
<i>Anyrun</i>	45

<i>Trendmicro</i>	45
CONFIGURAZIONE DEI CONNETTORI	46
CONFIGURAZIONE MANUALE	46
CONFIGURAZIONE TRAMITE CONTAINER DOCKER.....	47
CONFIGURAZIONE TRAMITE CONTAINER DOCKER VS MANUALE	48
WORKERS	49
CONFIGURAZIONE DI MISP ED ABILITAZIONE DEI FEED.....	51
CONFIGURAZIONE, SVILUPPO E TESTING DEL CONNETTORE ANYRUN.....	56
CONFIGURAZIONE, SVILUPPO E TESTING DEL CONNETTORE TREND MICRO	60
EXPORT DEI DATI	66

OpenCTI

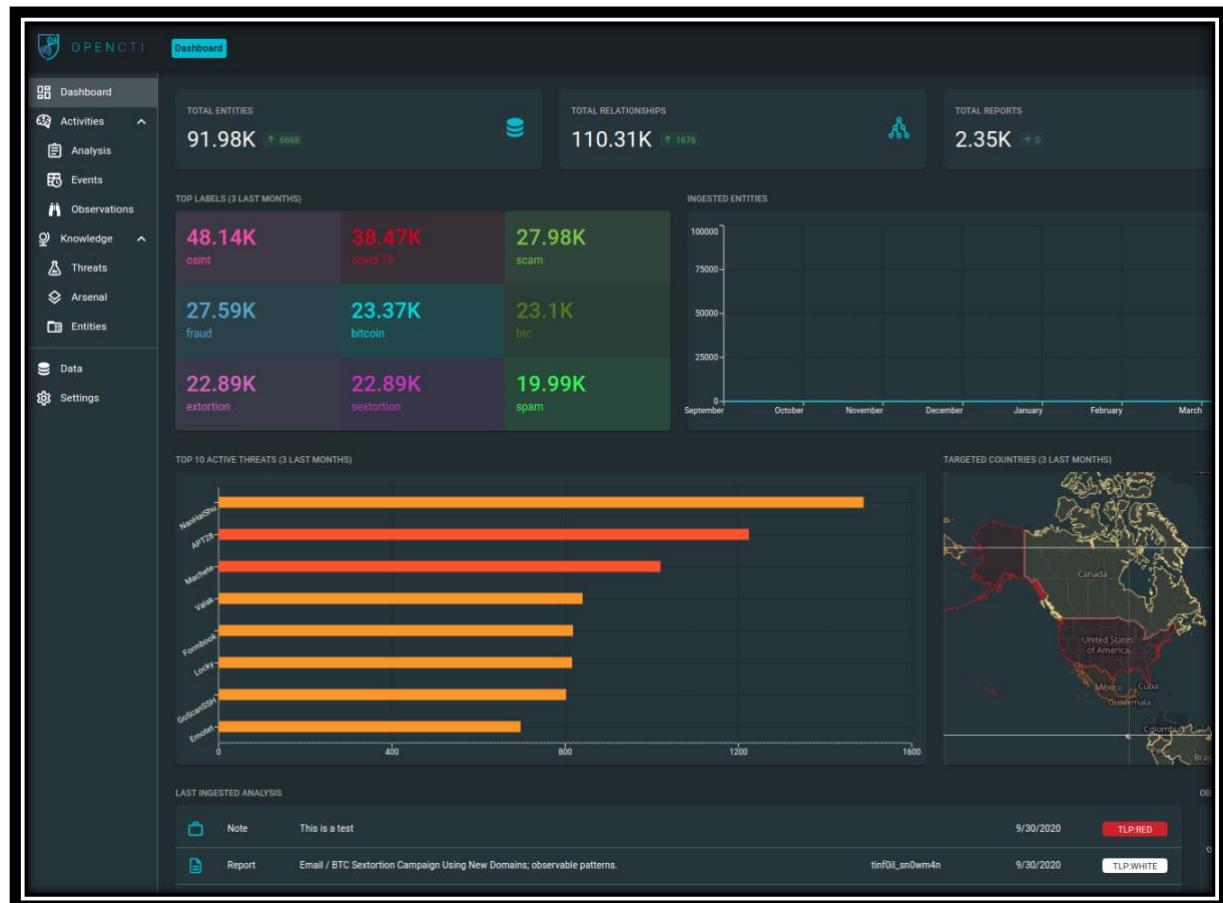
OpenCTI è una piattaforma open source che consente a qualsiasi utente o organizzazione di gestire le proprie informazioni sulle minacce informatiche. È stato creato per strutturare, archiviare e visualizzare informazioni tecniche e non tecniche sulle minacce informatiche.

I dati sono strutturati utilizzando uno schema di conoscenza basato sugli standard STIX2.

Le varie entità sono organizzate gerarchicamente e possono essere abstract entity, cioè entità base caratterizzate da un insieme di attributi e sub-entity, ossia entità che estendono quelle di tipo abstract, ereditandone gli attributi.

La piattaforma è stata progettata come una moderna applicazione web per cui, alla sua apertura la prima schermata che compare è la dashboard, la quale raggruppa tutti I dati principali.

OpenCTI include l'API GraphQL e può essere integrata con altri tools e/o applicazioni come MISP, TheHive, etc.



Dashboard di OpenCTI

Scopo

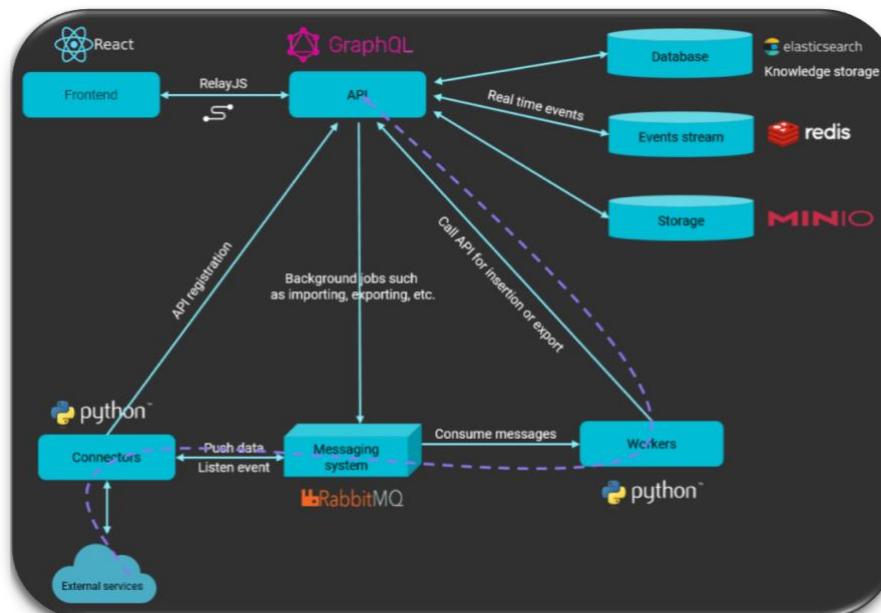
Questa piattaforma nasce con lo scopo di consentire agli utenti di archiviare e visualizzare informazioni tecniche (come TTP e osservabili) e informazioni non tecniche (come attribuzione suggerita, vittimologia, settore di attività e localizzazione), permettere di collegare ogni informazione alla sua fonte (un report, un evento MISP, etc) e fornire funzionalità come date di prima e ultima visualizzazione, collegamenti tra le informazioni, etc. OpenCTI sfrutta, tramite connettori dedicati, il framework MITRE ATT&CK, ossia una base di informazioni e conoscenze, accessibile gratuitamente da chiunque, di tattiche e tecniche ostili basate su osservazioni del mondo reale. MITRE ATT&CK viene utilizzato come base per lo sviluppo di modelli di cyber threats validi sia nel settore privato che in quello pubblico e governativo per migliorare i servizi di sicurezza informatica.

L'utente può anche scegliere di implementare i propri set di dati. Una volta che i dati sono stati integrati all'interno di OpenCTI, è possibile elaborarli per ricavare nuove relazioni e informazioni al fine di facilitare la comprensione e la rappresentazione dei dati stessi. OpenCTI consente non solo di importare i dati, ma anche di esportarli in diversi formati (CSV, STIX2 bundles, etc).

Architettura

Per il suo funzionamento, la piattaforma OpenCTI si basa su vari componenti.

- **API GraphQL:** è la parte centrale della piattaforma OpenCTI, consentendo ai client di interagire con il database e il sistema di messaggistica, implementato con il broker RabbitMQ. È costruito in NodeJS e implementa il linguaggio di query GraphQL.
- **Database:** serve per archiviare le informazioni e le conoscenze acquisite. È implementato con ElasticSearch.
- **Workers:** sono processi Python autonomi che consumano messaggi dal broker per eseguire query di scrittura asincrona. È possibile avviare tutti I workers di cui si necessita per incrementare le scritture parallele e quindi il throughput. Ciò, ovviamente, è possibile finché non si raggiungerà il punto di saturazione rappresentato dal throughput del database.
- **Connettori:** sono processi Python di terze parti che possono svolgere 5 ruoli differenti:
 1. **EXTERNAL_IMPORT:** estraggono i dati da fonti remote, li convertono in STIX2 e li importano su OpenCTI.
 2. **INTERNAL_IMPORT_FILE:** estraggono i dati dai file caricati su OpenCTI tramite la GUI o l'API.
 3. **INTERNAL_ENRICHMENT:** rimangono in attesa di eventi relativi a nuove entità o a richieste degli utenti, per poi estrarre i dati allo scopo di arricchirli
 4. **INTERNAL_EXPORT_FILE:** esportano i dati da OpenCTI, sulla base delle varie entità definite e delle loro relazioni.
 5. **STREAM CONSUMER:** consumano i dati della piattaforma.



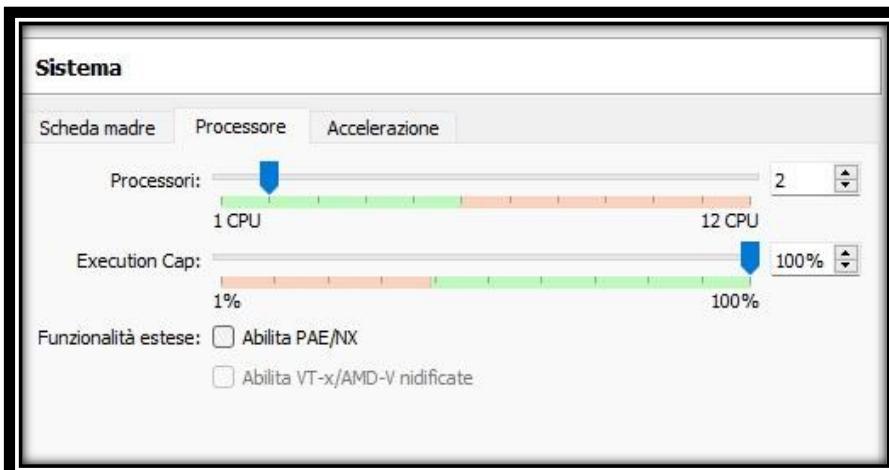
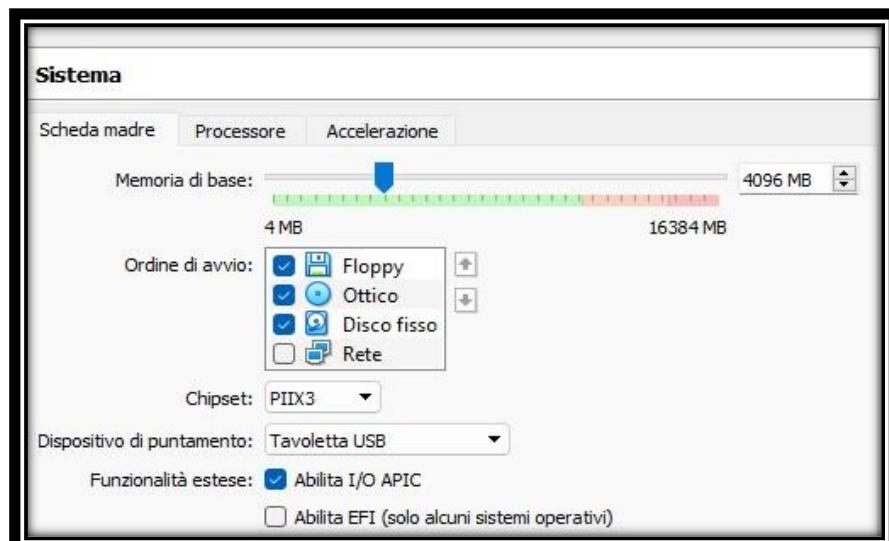
Installazione e configurazione di OpenCTI

OpenCTI può essere installata manualmente, su macchine con Ubuntu come sistema operativo, oppure attraverso procedure automatizzate che richiedono l'uso di una Virtual Machine o di Docker. Per semplicità si è deciso di optare per un'installazione automatizzata basata su una macchina virtuale, con Virtual Box come HyperVisor di tipo 2.

Anzitutto occorre effettuare il download del file OVA «opencti-release-5.0.3.ova» reperibile al link: https://drive.google.com/drive/folders/1bvB6RmdQNHMW_3h-88KbAit9GRZIL5Bj.

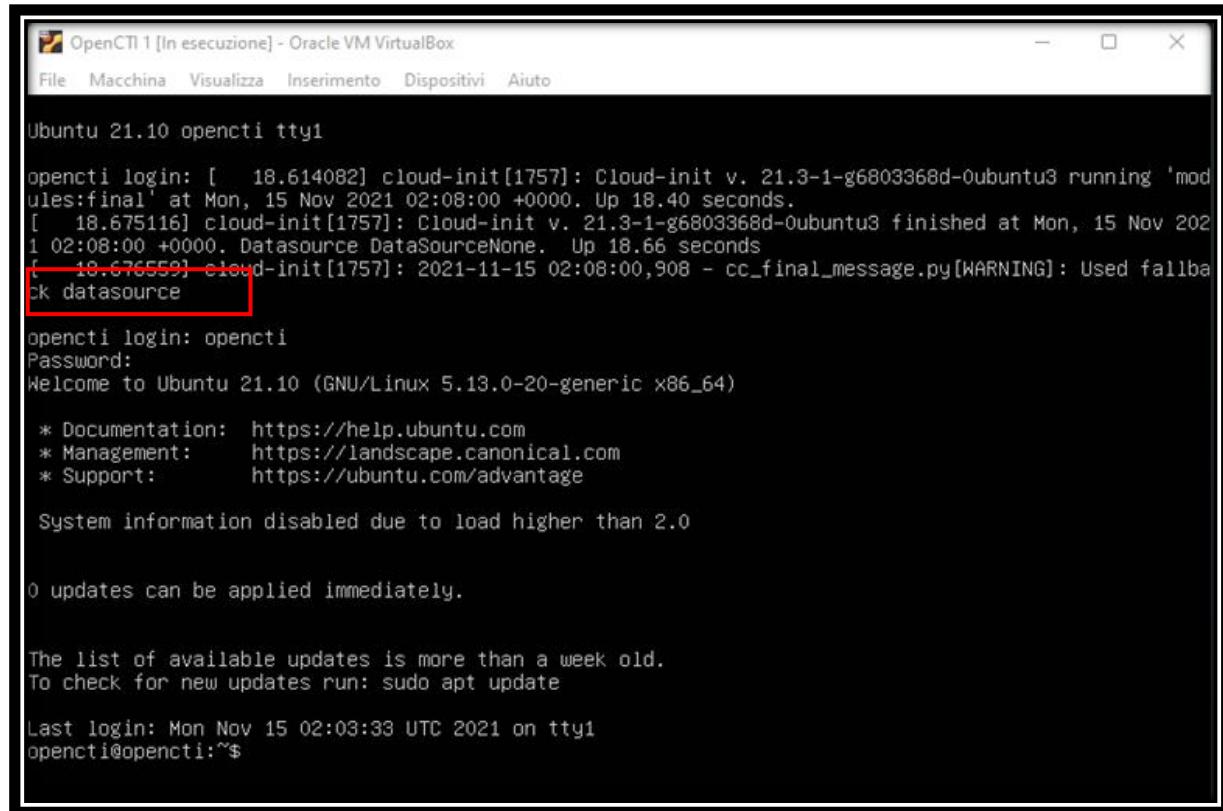
Questo file potrà, poi, essere importato in Virtual Box per generare automaticamente una macchina virtuale preconfigurata.

Inoltre, siccome la VM è preconfigurata con 1 core per la CPU e 16 GB di memoria RAM, al fine di garantire prestazioni migliori ed evitare di concedere più memoria di quella necessaria, le risorse assegnate alla macchina sono state modificate in 2 core e 4 GB di RAM.



Una volta avviata la VM è necessario effettuare l'accesso usando le credenziali di login:

- Username: opentcti
- Password: opentcti



```
OpenCTI 1 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Ubuntu 21.10 opentcti tty1

opentcti login: [ 18.614082] cloud-init[1757]: Cloud-init v. 21.3-1-g6803368d-0ubuntu3 running 'modules:final' at Mon, 15 Nov 2021 02:08:00 +0000. Up 18.40 seconds.
[ 18.675116] cloud-init[1757]: Cloud-init v. 21.3-1-g6803368d-0ubuntu3 finished at Mon, 15 Nov 2021 02:08:00 +0000. Datasource DataSourceNone. Up 18.66 seconds
[ 18.676559] cloud-init[1757]: 2021-11-15 02:08:00,908 - cc_final_message.py[WARNIN]: Used fallba
ck datasource

opentcti login: opentcti
Password:
Welcome to Ubuntu 21.10 (GNU/Linux 5.13.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information disabled due to load higher than 2.0

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

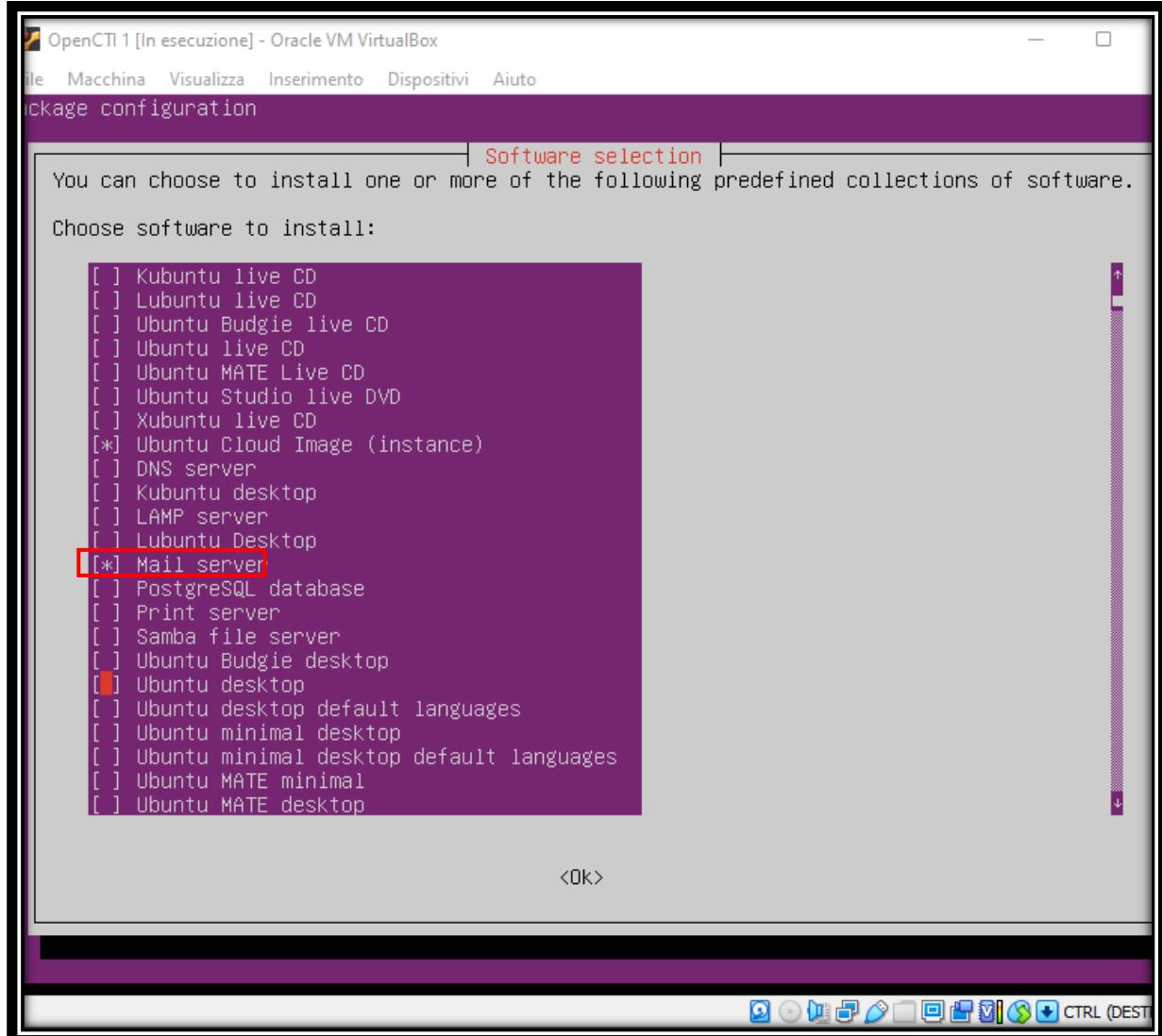
Last login: Mon Nov 15 02:03:33 UTC 2021 on tty1
opentcti@opentcti:~$
```

In questa fase, la VM è sprovvista sia di un browser che di un tool per reperire il proprio indirizzo IP, entrambi necessari per accedere alla dashboard di OpenCTI dalla VM stessa. Dunque, per permettere ciò, il successivo step della configurazione consisterà nella loro installazione.

Per installare i componenti mancanti è sufficiente eseguire i seguenti comandi:

1. *sudo apt-get upgrade*
2. *sudo apt-get update*
3. *sudo apt install net-tools* (consente di utilizzare il comando ifconfig, necessario per ricavare il proprio indirizzo IP)
4. *sudo apt install tasksel* (necessario per installare una GUI con cui sarà possibile utilizzare un browser, a sua volta necessario per visualizzare la dashboard di OpenCTI)
5. *sudo apt install slim* (display manager per poter visualizzare la GUI)
6. *sudo tasksel*

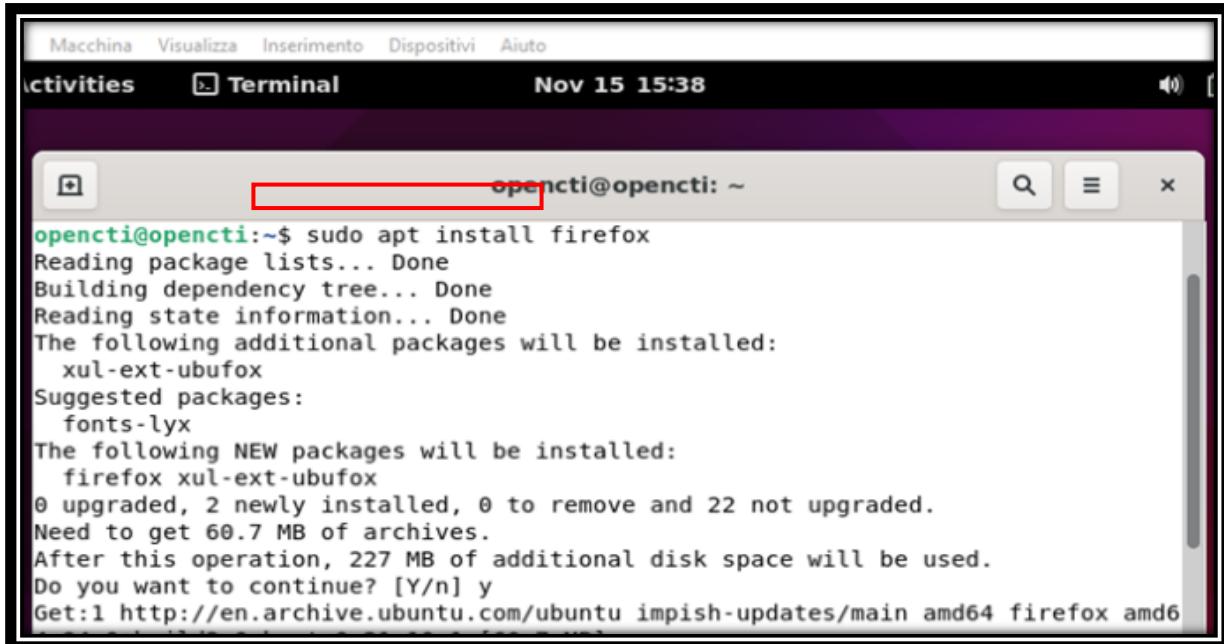
Eseguendo l'ultimo comando comparirà un'interfaccia tramite la quale sarà possibile scegliere quale GUI installare. Per semplicità è stata selezionata l'interfaccia più essenziale disponibile, ossia Ubuntu Desktop.



Al termine dell'installazione bisognerà riavviare la VM.

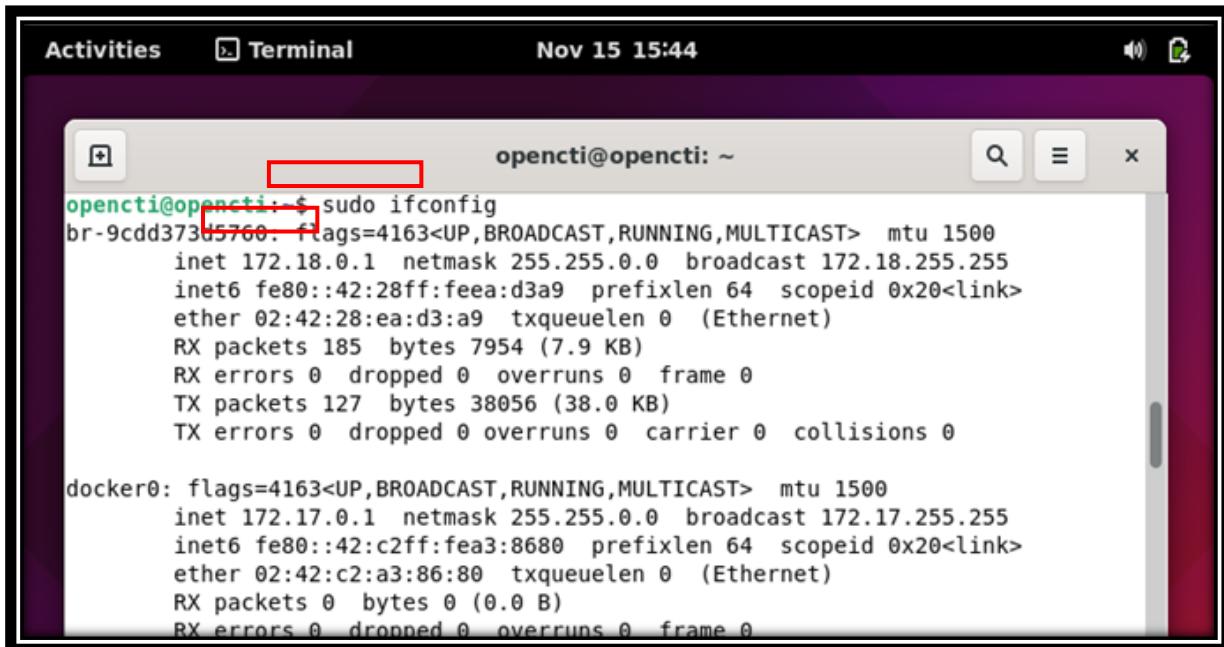
Da questo momento in poi, ogni volta che si avvierà la VM, verrà effettuato l'accesso ad Ubuntu automaticamente tramite la GUI e non più dalla shell di comando.

Una volta avviata la VM da GUI sarà necessario installare un browser per visualizzare la dashboard di OpenCTI. Per convenzione si è deciso di installare Firefox, per cui è sufficiente aprire la shell ed eseguire il comando `sudo apt install firefox`.



```
Macchina Visualizza Inserimento Dispositivi Aiuto
Activities Terminal Nov 15 15:38
opencti@opencti: ~
opencti@opencti:~$ sudo apt install firefox
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  xul-ext-ubufox
Suggested packages:
  fonts-lyx
The following NEW packages will be installed:
  firefox xul-ext-ubufox
0 upgraded, 2 newly installed, 0 to remove and 22 not upgraded.
Need to get 60.7 MB of archives.
After this operation, 227 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://en.archive.ubuntu.com/ubuntu impish-updates/main amd64 firefox amd64
```

A questo punto bisogna recuperare il proprio indirizzo IP, il che può essere fatto tramite il comando `sudo ifconfig`. L'IP da utilizzare sarà il primo restituito dal comando, ossia 172.18.0.1.



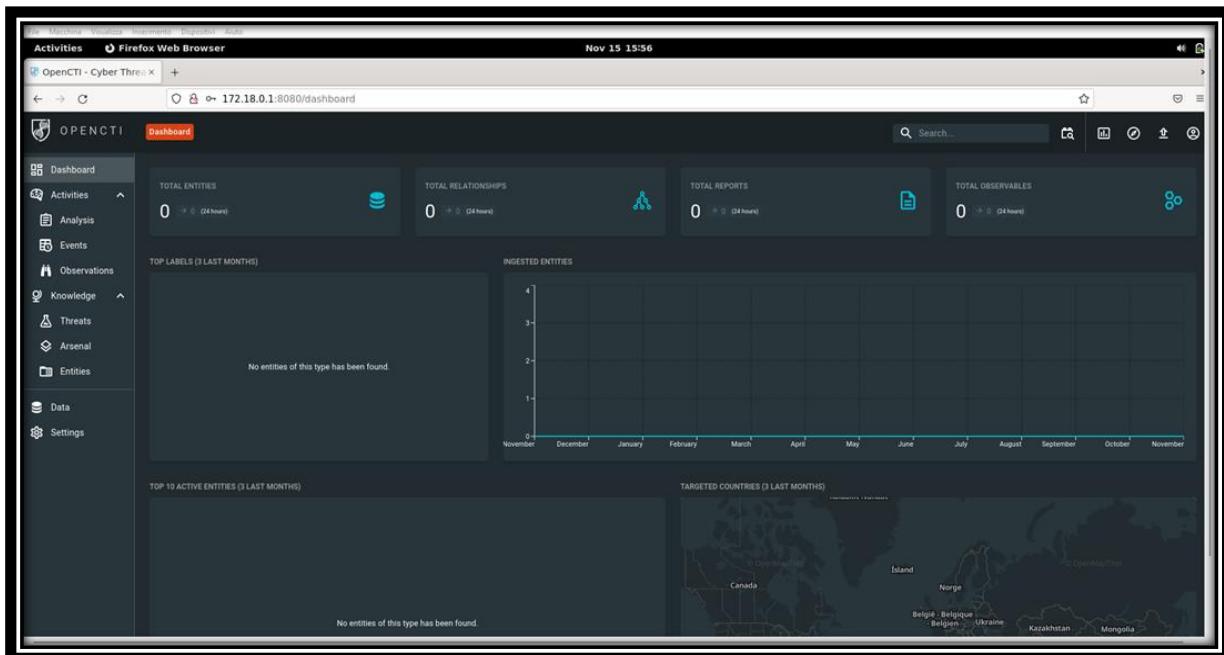
```
Activities Terminal Nov 15 15:44
opencti@opencti: ~
opencti@opencti:~$ sudo ifconfig
br-9cdd373d5760: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
    inet6 fe80::42:28ff:fea:d3a9 prefixlen 64 scopeid 0x20<link>
      ether 02:42:28:ea:d3:a9 txqueuelen 0 (Ethernet)
        RX packets 185 bytes 7954 (7.9 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 127 bytes 38056 (38.0 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:c2ff:fea3:8680 prefixlen 64 scopeid 0x20<link>
      ether 02:42:c2:a3:86:80 txqueuelen 0 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
```

Dopodiché, occorre eseguire il comando `sudo -p 22 opencti@172.18.0.1` per impostare questo IP come affidabile.

Infine, si deve aprire il browser e contattare il seguente URL: <http://172.18.0.1:8080> (questa operazione può essere effettuata solo dopo il termine dell'avvio della piattaforma, cosa che richiede mediamente 5 minuti da quando si accede alla VM). Si verrà reindirizzati alla schermata di login di OpenCTI, dove si potranno utilizzare le seguenti credenziali per accedere alla dashboard:

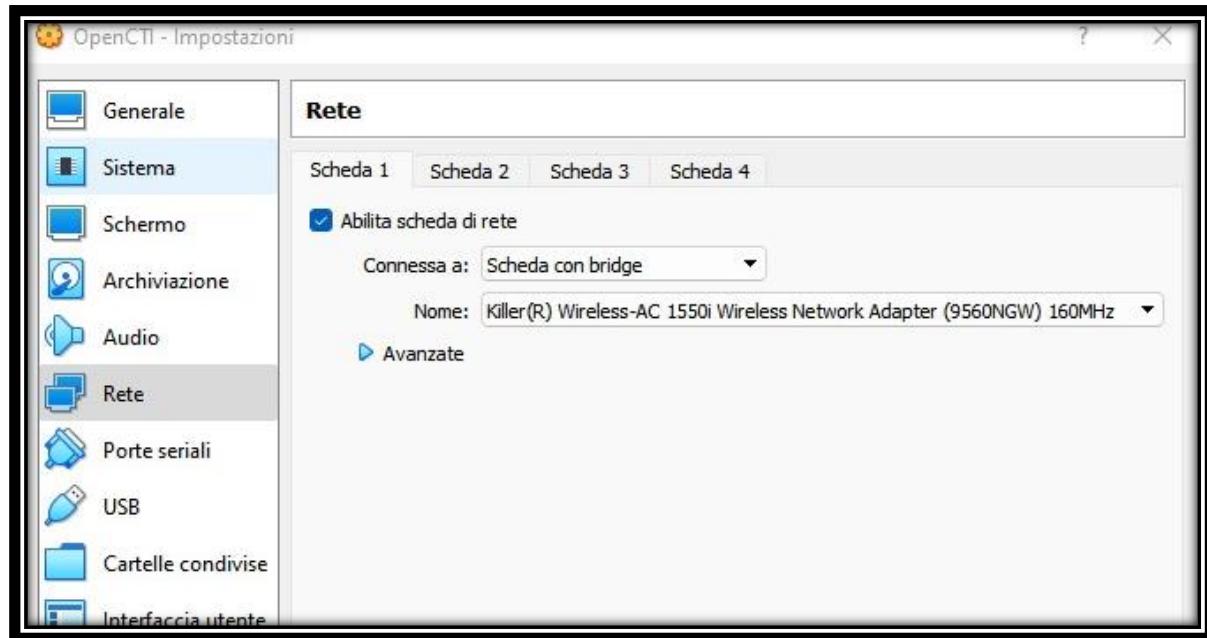
- Username: admin@opencti.io
- Password: admin



A questo punto la VM è completamente configurata ed è possibile utilizzarla anche per accedere, tramite essa, alla dashboard di OpenCTI.

In realtà, è possibile accedere alla dashboard anche tramite browser di altre machine, come l'host della VM o uno smartphone. Per un'ottimizzazione delle risorse, oltre ad aver seguito i passaggi illustrati precedentemente, sono state effettuate anche delle ulteriori operazioni, al fine di raggiungere questo risultato.

Anzitutto, in Virtual Box, la connessione della VM è stata opportunamente modificata da *NAT* a *Scheda con Bridge*.



Poi, dalla shell di comando, è stato usato nuovamente il comando `sudo -p 22 opencti@172.18.0.1`, questa volta con lo scopo di recuperare l'indirizzo IP da usare per accedere alla dashboard da un'altra macchina.

```
opencti@opencti:~$ ssh -p 22 opencti@172.18.0.1
opencti@172.18.0.1's password:
Welcome to Ubuntu 21.10 (GNU/Linux 5.13.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information disabled due to load higher than 3.0

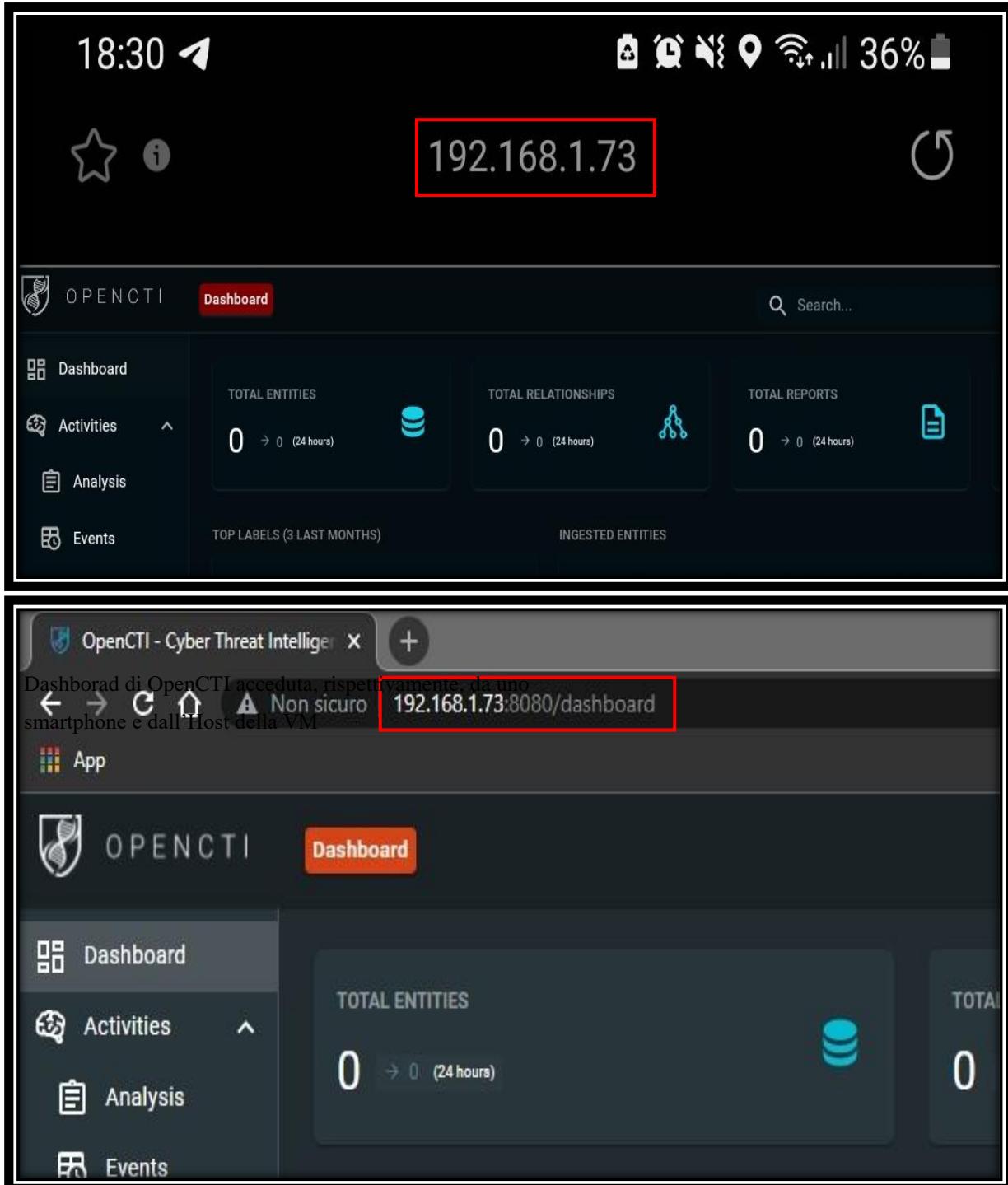
 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.

Last login: Wed Nov 17 16:54:56 2021 from 192.168.1.73
opencti@opencti:~$ █
```

Arrivati a questo punto, sarà possibile accedere alla dashboard di OpenCTI anche tramite altre macchine, ricordando, ovviamente, di usare il nuovo IP per comporre l'URL da contattare via browser.



API clients

Per quanto riguarda i clients di OpenCTI, è possibile scriverli in 2 diversi linguaggi di programmazione:

- Python
- Go

Client in Python

Con Python, l'interazione con OpenCTI avviene tramite la libreria pycti.

- Prerequisiti: Python >= 3
- Installazione: è richiesta l'installazione dell'ultima versione della libreria pycti tramite il comando `pip3 install pycti`

```
from dateutil.parser import parse
from pycti import OpenCTIApiClient
from stix2 import TLP_GREEN

# OpenCTI API client initialization
opencti_api_client = OpenCTIApiClient("https://myopencti.server", "mysupersecrettoken")

# Define an OpenCTI compatible date
date = parse("2019-12-01").strftime("%Y-%m-%dT%H:%M:%SZ")

# Get the OpenCTI marking for stix2 TLP_GREEN
TLP_GREEN_CTI = opencti_api_client.marking_definition.read(id=TLP_GREEN["id"])

# Use the client to create an indicator in OpenCTI
indicator = opencti_api_client.indicator.create(
    name="C2 server of the new campaign",
    description="This is the C2 server of the campaign",
    pattern_type="stix",
    indicator_pattern="[domain-name:value = 'www.5z8.info']",
    x_opencti_main_observable_type="IPv4-Addr",
    valid_from=date,
    update=True,
    markingDefinitions=[TLP_GREEN_CTI["id"]],
)
```

Esempio di inizializzazione di un client e creazione di un indicatore

È possibile trovare ulteriore documentazione, per la libreria pycti, al seguente link: opencti-client-for-python.readthedocs.io.

Client in Go

Nella documentazione di OpenCTI non è riportata alcuna informazione relativa alla creazione e all'utilizzo di un client scritto in Go.

Connettori OpenCTI

In questa sezione saranno descritti alcuni connettori (già sviluppati o ancora in fase di sviluppo) che è possibile collegare alla piattaforma e che consentono, a loro volta, di integrare altri tools o altre applicazioni.

Per la maggioranza dei connettori è disponibile sia il codice sorgente (che è essenzialmente uno script scritto in Python) sia un'immagine docker, che consente di effettuare il deploying in modo veloce.

Esistono due modi per integrare un connettore con OpenCTI:

- avviando il processo Python direttamente dopo aver fornito la configurazione corretta nel file config.yml
- attraverso un container docker

Data import

AlienVault

Può essere utilizzato per importare la conoscenza dalla piattaforma Alien Labs Open Threat Exchange (OTX).

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	<p>È richiesta l'adesione alla community di intelligence sulle minacce OTX (AlienVault - Open Threat Exchange)</p> <p>Librerie:</p> <ul style="list-style-type: none">• pycti==5.0.3• pydantic==1.8.2• OTXv2==1.5.12	connectors/external-import/alienVault_at_master · OpenCTI-Platform/connectors · GitHub

AM!TT

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none"> • pycti==5.0.3 • urllib3==1.26.5 • python-dateutil==2.8.1 	connectors/external-import/amitt_at/master.py · OpenCTI-Platform/connectors · GitHub

CAPE Sandbox

Questo è un connettore per sincronizzare l'analisi sandbox CAPE come report e IOC OpenCTI.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	<ul style="list-style-type: none"> • OpenCTI Platform >= 5.1.0 • pycti==5.0.3 • certifi==2021.5.30 • chardet==4.0.0 • datefinder==0.7.1 • idna==2.10 • python-dateutil==2.8.1 • pytz==2021.1 • regex==2021.8.28 • simplejson==3.17.5 • six==1.16.0 • stix2-patterns==1.3.2 • urllib3==1.26.6 	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/cape

CrowdStrike

Il connettore OpenCTI CrowdStrike può essere utilizzato per importare conoscenza dalla piattaforma CrowdStrike Falcon. Il connettore sfrutta le API Intel per ottenere informazioni sull'intelligence di CrowdStrike, inclusi dati su attori, indicatori, report e regole YARA.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	Richiede l'abbonamento alla piattaforma CrowdStrike Falcon. Inoltre, sono richieste le credenziali RabbitMQ (vengono fornite direttamente dell'API). Librerie: <ul style="list-style-type: none">• pycti==5.0.3• lxml==4.6.3 https://github.com/certeu/crowdstrike-client#egg=crowdstrike-client	connectors/external-import/crowdstrike at master · OpenCTI-Platform/connectors · GitHub

Cryptolaemus

I membri di Cryptolaemus condividono informazioni in modo tale che tutti possano importare gli IOC nei loro prodotti di sicurezza informatica e proteggerli da possibili infezioni da Emotet, o aiutare con rilevamenti precoci prima che il malware possa causare danni ingenti.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5• python-dateutil==2.8.1• feedparser==6.0.2• beautifulsoup4==4.9.3• lxml==4.6.3	connectors/external-import/cryptolaemus at master · OpenCTI-Platform/connectors · GitHub

Cuckoo Sandbox

Cuckoo Sandbox è il principale sistema di analisi malware automatizzato open source. Puoi lanciare qualsiasi file sospetto in un ambiente sandbox e in pochi minuti Cuckoo fornirà un rapporto dettagliato che delinea il comportamento del file. È un software gratuito che automatizza l'attività di analisi di qualsiasi file dannoso in Windows, macOS, Linux e Android. Il repository non è al momento raggiungibile.

CVE Database

L'NVD è l'archivio del governo degli Stati Uniti di dati di gestione delle vulnerabilità. L'NVD include database di riferimenti a elenchi di controllo di sicurezza, difetti software relativi alla sicurezza, configurazioni errate, nomi di prodotti e metriche di impatto.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5• certifi==2020.6.20	connectors/external-import/cve at master · OpenCTI-Platform/connectors · GitHub

Cyber Threat Coalition (COVID-19)

Il connettore OpenCTI Cyber Threat Coalition importa gli indicatori pubblicati dal team Cyber Threat Coalition. Cyber Threat Coalition è un team di esperti che raccolgono e condividono informazioni sulle minacce informatiche legate alla pandemia durante il periodo di crisi del COVID-19

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• feedparser==6.0.2	connectors/external-import/cyber-threat-coalition at master · OpenCTI-Platform/connectors · GitHub

Cybercrime Tracker

Il connettore utilizza il feed RSS del tracker in: <http://cybercrime-tracker.net/rss.xml>.

Genera un indicatore per ogni voce, indicando il relativo malware.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• feedparser==6.0.2• pygrok==1.0.0	connectors/external-import/cybercrime-tracker at master · OpenCTI-Platform/connectors · GitHub

Files restore

Questo connettore consente alle organizzazioni di ripristinare i propri dati OpenCTI da una cartella specifica.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti==5.0.3• una directory accessibile dallo script Python con accesso in scrittura	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/restore-files

FireEye

Questo connettore si collega all'API FireEye Intel V3 e raccoglie tutti i dati a partire da una determinata data.

Integrabile	API	Requisiti	Link al repository GitHub
Non è detto che la versione free sia integrabile.	OPEN la versione free.	Librerie: <ul style="list-style-type: none">• pycti==5.0.3	connectors/external-import/fireeye_at master · OpenCTI-Platform/connectors · GitHub

Kaspersky

Il connettore OpenCTI Kaspersky può essere utilizzato per importare la conoscenza da Kaspersky Threat Intelligence Portal. Il connettore sfrutta l'API del portale di Kaspersky Threat Intelligence per recuperare le informazioni pubblicate sul portale di Kaspersky Threat Intelligence, inclusi PDF di report, IoC e regole YARA.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	Licenza per utilizzare i servizi di Kaspersky Threat Intelligence Portal Librerie: <ul style="list-style-type: none">• pycti==5.0.3• pydantic==1.8.2• lxml==4.6.3	connectors/external-import/kaspersky_at master · OpenCTI-Platform/connectors · GitHub

LastInfoSec

Il connettore OpenCTI LastInfoSec utilizza l'API /v2/stix21/getlasthour. Questo feed di minacce di LastInfosec contiene rapporti STIXv2.1 aggiornati ogni ora con URL, hash, indicatori di domini.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	Necessaria una chiave API (https://info.gatewatcher.com/en/lp/opencti). Librerie: <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5	connectors/external-import/lastinfosec at master · OpenCTI-Platform/connectors · GitHub

Malpedia

Questo connettore importa la conoscenza dalla libreria di Malpedia. Il connettore aggiunge dati per i seguenti tipi di indicatore/osservabile OpenCTI:

- Yara
- file-sha256

Si prega di notare che Malpedia è gestito come un gruppo dove si accede solo su invito. Di conseguenza ogni registrazione sarà sottoposta a verifica.

L'accesso alle sole informazioni pubbliche può essere effettuato settando TLP:WHITE. Solo in questo caso non sarà richiesto un account.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API OPEN per informazioni pubbliche.	Necessaria una chiave API (https://malpedia.caad.fkie.fraunhofer.de/settings). Librerie: <ul style="list-style-type: none">• pycti==5.0.3• pydantic==1.8.2	connectors/external-import/malpedia at master · OpenCTI-Platform/connectors · GitHub

MISP

Questo connettore importa la conoscenza dalla libreria di Malpedia. Il connettore aggiunge dati per i seguenti tipi di indicatore/osservabile OpenCTI:

- Yara
- file-sha256

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	<p>Credenziali RabbitMQ (vengono fornite direttamente dell'API).</p> <p>Librerie:</p> <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5• pymisp• python-dateutil==2.8.1• stix2==2.1.0	connectors/external-import/misp_at_master · OpenCTI-Platform/connectors · GitHub

MITRE ATT&CK

MITRE ATT&CK è una base di conoscenza accessibile a livello globale di tattiche e tecniche avversarie basate su osservazioni del mondo reale. La base di conoscenza ATT&CK viene utilizzata come base per lo sviluppo di modelli e metodologie di minaccia specifici nel settore privato, nel governo e nella comunità di prodotti e servizi di sicurezza informatica.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	<p>Librerie:</p> <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5• certifi==2020.12.5	connectors/external-import/mitre_at_master · OpenCTI-Platform/connectors · GitHub

OpenCTI datasets

Il seguente repository viene utilizzato per archiviare i campioni di dati OpenCTI utilizzati dai connettori OpenCTI per sincronizzare i cataloghi di settori, regioni e paesi.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5	connectors/external-import/opencti at master · OpenCTI-Platform/connectors · GitHub

RiskIQ

Il connettore OpenCTI RiskIQ può essere utilizzato per importare la conoscenza dall'API RiskIQ.

Il connettore importa gli articoli di RiskIQ. Un articolo viene archiviato come un report STIX, contenente più indicatori.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN piano base.	Probabilmente è richiesta registrazione. Librerie: <ul style="list-style-type: none">• pycti==5.0.3• stix2==2.1.0• urllib3==1.26.6	connectors/external-import/riskiq at master · OpenCTI-Platform/connectors · GitHub

Sekoia

SEKOIA.IO integra i flussi di intelligence degli aggressori e le capacità di automazione per identificare, comprendere e neutralizzare gli attacchi più rapidamente.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	Probabilmente è richiesta registrazione. Librerie: <ul style="list-style-type: none">• pycti==5.0.3• python-dateutil==2.8.1	connectors/external-import/sekoia at master · OpenCTI-Platform/connectors · GitHub

TAXII2

Importa i bundle STIX2.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Probabilmente è richiesta registrazione. Librerie: <ul style="list-style-type: none">• pycti==5.0.3• antlr4-python3-runtime• certifi• chardet• datefinder• idna• pika• python-dateutil• python-magic• pytz• PyYAML• regex	connectors/external-import/taxii2 at master · OpenCTI-Platform/connectors · GitHub

		<ul style="list-style-type: none"> • requests • simplejson • six • sseclient • stix2 • stix2-patterns • taxii2-client • urllib3 	
--	--	---	--

TheHive

È una piattaforma di risposta agli incidenti di sicurezza scalabile, open source e gratuita. Fornisce informazioni relative ai security incidents.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Probabilmente è richiesta registrazione. Librerie: <ul style="list-style-type: none"> • pycti==5.0.3 • thehive4py 	connectors/external-import/thehive at master · OpenCTI-Platform/connectors · GitHub

ThreatMatch

Garantisce la consegna di rapporti periodici sulle minacce, rapporti e ricerche personalizzate sui clienti, inclusi collegamenti ad avvisi, incidenti, profili e scenari. I rapporti sulle minacce vengono forniti come parte dell'abbonamento a ThreatMatch.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	Vengono richieste le credenziali RabbitMQ (vengono fornite direttamente dell'API). Probabilmente è richiesta registrazione. Librerie: <ul style="list-style-type: none">• pycti==5.0.3	connectors/external-import/threatmatch at master · OpenCTI-Platform/connectors · GitHub

URLhause by Abuse.ch

URLhaus è un progetto di abuse.ch con l'obiettivo di condividere URL dannosi che vengono utilizzati per la distribuzione di malware.

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN	Librerie: <ul style="list-style-type: none">• pycti==5.0.3• urllib3==1.26.5• certifi==2020.6.20	connectors/external-import/urlhaus at master · OpenCTI-Platform/connectors · GitHub

Valhalla

Questo connettore importa la conoscenza dall'API Valhalla. Il connettore aggiunge dati per i seguenti tipi di indicatore/osservabile Valhalla:

- modello indicatore stix2: yara

Il set di regole demo (noto anche come signature-base) contiene regole gratuite con licenza CC-BY-NC. L'accesso completo al database delle regole richiede un abbonamento attivo. Gli abbonamenti possono essere richiesti da <https://www.nextron-systems.com/valhalla/>

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN PIANO BASE	Abbonamento attivo per versione full. Librerie: <ul style="list-style-type: none">• pycti==5.0.3• pydantic==1.8.2• valhallaAPI==0.3.0	connectors/external-import/valhalla_at_master · OpenCTI-Platform/connectors · GitHub

Virustotal Livehunt

Integrabile	API	Requisiti	Link al repository GitHub
SI	OPEN VERSIONE DEMO	Librerie: <ul style="list-style-type: none">• pycti==5.1.2• vt-py==0.8.0	https://github.com/OpenCTI-Platform/connectors/tree/master/external-import/virustotal-livehunt-notifications

VX Vault

Repository non raggiungibile.

Yeti

Repository non disponibile.

Stream consumer

Backup Files

Questo connettore consente alle organizzazioni di prendere i propri dati OpenCTI e scriverli in una cartella specifica (di backup).

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• una directory accessibile dallo script Python con accesso in scrittura.• pycti==5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/backup-files

Elastic

Questo connettore consente alle organizzazioni di alimentare la propria piattaforma elastica utilizzando la conoscenza di OpenCTI. Ha due modalità: ecs e stix. Questo connettore utilizza il flusso di eventi OpenCTI, quindi prende la conoscenza (le info) in tempo reale e aggiorna i documenti degli indicatori in formato ECS.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• Elastic platform >= 7.14.0• elasticsearch==7.13.1• Python3.9.x	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/elastict

History

Questo connettore utilizza il flusso OpenCTI e scrive la cronologia delle entità. I connettori della cronologia memorizzano la configurazione attiva più recente di uno stato e dei relativi sottostati. Una volta creato, un oggetto viene associato a una configurazione per uno stato attivo, a partire dalla configurazione iniziale, e poi evolve man mano che il diagramma di stato risponde ai messaggi.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti==5.0.3• elasticsearch==7.13.1	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/history

QRadar

Questo connettore è in grado di stabilire una correlazione tra tutte le varie informazioni e di raggruppare gli eventi correlati in singoli avvisi al fine di accelerare l'analisi e la correzione degli incidenti. Il repository GitHub non è disponibile.

Splunk

È un connettore OpenCTI che importa eventi da Splunk Enterprise.

Questo connettore prende tutti gli eventi STIX2 memorizzati in un indice e li importa in OpenCTI.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti==5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/splunk

Tanium

Questo connettore consente alle organizzazioni di alimentare uno Splunk KV Store utilizzando la conoscenza di OpenCTI. Dopo aver avviato il connettore, si dovrebbe essere in grado di vedere una nuova fonte di Intelligence all'interno della piattaforma Tanium:

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	API PAGAMENTO A	<ul style="list-style-type: none"> • OpenCTI Platform >= 5.0.0 • Tanium Threat Response >= 3.X.X • pycti == 5.0.3 • ioc_writer == 0.3.3 • stix2-slider==3.0.0 	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/splunk

Tenzir→ThreatBus

Questo connettore consente la comunicazione tra OpenCTI e Threat Bus, il livello di diffusione dell'intelligence sulle minacce per gli strumenti di sicurezza open source. Utilizzando questo connettore, si può integrare profondamente OpenCTI threat intelligence con strumenti di rilevamento e database, come VAST, Zeek o CIF-3. Come funziona:

Il connettore funge da imbuto bidirezionale per indicatori e avvistamenti (Sightings) STIX-2. Utilizza il flusso di eventi OpenCTI (SSE) per elaborare gli aggiornamenti degli indicatori in tempo quasi reale e inoltra gli indicatori STIX-2 a Threat Bus tramite ZeroMQ. Allo stesso tempo, il connettore si iscrive al Threat Bus Topic per STIX-2 Sightings. Ogni volta che vengono pubblicati nuovi avvistamenti sul bus, il connettore li inoltra a OpenCTI tramite chiamate API.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	API PAGAMENTO A	<ul style="list-style-type: none"> • un file di configurazione o determinate variabili di ambiente per l'avvio. • pycti == 5.0.3 • threatbus == 2021.6.24 • pyzmq==22.0.3 	https://github.com/OpenCTI-Platform/connectors/tree/master/stream/threatbus

Internal Enrichment

AbuseIPDB

È un database di indirizzi IP dannosi, coinvolti in attività dannose come spamming, tentativi di hacking, attacchi DDoS, ecc.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	1.000 controlli IP al giorno	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/abuseipdb

CAPE Sandbox

CAPE Sandbox è un software Open Source per automatizzare l'analisi dei file sospetti. Per fare ciò si avvale di componenti personalizzati che monitorano il comportamento dei processi dannosi durante l'esecuzione in un ambiente isolato.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	API A PAGAME NTO	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• pycti == 5.0.3• pyzipper==0.3.5	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/cape-sandbox

Gatewatcher Lastinfosec

Il feed delle minacce di LastInfoSec è un feed di dati che semplifica il rilevamento delle minacce all'interno del sistema informativo. Contiene evidenze compromesse arricchite al fine di ridurre il tempo di analisi delle minacce una volta rilevate. LastInfoSec è stato creato per facilitare il rilevamento delle intrusioni nella tua azienda o organizzazione attraverso un feed di Threat Intelligence basato sull'intelligenza artificiale e la nostra esperienza nella risposta agli incidenti.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	Bisogna richiederla: https://info.gatewatcher.com/en/lp/opencti	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/lastinfosec

GreyNoise

È un sistema che raccoglie, analizza ed etichetta la scansione Internet omnidirezionale e l'attività di attacco. Lo scopo di questo connettore è rispondere a questa domanda: "Tutti gli altri vedono queste cose o sono solo io che le vedo?" In altre parole: "Si tratta solo di un normale rumore di fondo di Internet o la macchina sta effettivamente mirando e attaccando ME in modo specifico?". Il connettore GreyNoise è un processo Python autonomo che deve avere accesso alla piattaforma OpenCTI e RabbitMQ. Le credenziali RabbitMQ e i parametri di connessione sono forniti direttamente dall'API, come configurato nelle impostazioni della piattaforma. L'abilitazione di questo connettore può essere eseguita avviando il processo Python direttamente dopo aver fornito la configurazione corretta nel file config.yml o all'interno di un Docker con l'immagine opencti/connector-greynoise:latest.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN, versione demo	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycountry==20.7.3• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/greynoise

Hatching Triage Sandbox

Una sandbox di malware. Triage è la nuova e rivoluzionaria soluzione sandbox di malware di Hatching. Sfrutta un'architettura unica, sviluppata pensando alla scalabilità fin dall'inizio. Il triage può scalare fino a 500.000 analisi al giorno, un numero senza precedenti per un servizio di sandboxing.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO, con versione demo	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• hatching-triage==0.1.4• git+git://github.com/OpenCTI-Platform/client-python	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/hatching-triage-sandbox

Hybrid Analysis

Questo è un servizio di analisi malware, gratuito per la comunità, che rileva e analizza le minacce sconosciute utilizzando un'esclusiva tecnologia di analisi ibrida.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/hybrid-analysis-sandbox

Hygiene

Questo è un connettore di arricchimento interno che utilizza i seguenti progetti esterni per cercare valori osservabili nel database che potresti voler eliminare perché è noto che portano ad alse-positivi quando vengono utilizzati per il rilevamento. [misp-warninglists](#)

Il connettore funziona per i seguenti tipi osservabili OpenCTI:

- Indirizzo IPv4
- Indirizzo IPv6
- Nome del dominio
- StixFile
- Artefatto

L'abilitazione di questo connettore può essere eseguita avviando il processo Python direttamente dopo aver fornito la configurazione corretta nel file config.yml o all'interno di un Docker con l'immagine opencti/connector-hygiene:latest.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	Limitazione giornaliera sul numero di query.	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• https://github.com/MISP/PyMISPWarningLists	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/hygiene

Import External Reference

Questo connettore consente alle organizzazioni di importare riferimenti esterni come file PDF o file MarkDown.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3• weasyptint == 53.2• html2text == 2020.1.16• pdfminer.six == 20201018• pdfkit == 0.6.1	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/import-external-reference

Intezer Sandbox

Il più grande database di minacce genetiche per tenere traccia delle varianti e degli attori delle minacce più recenti.

Integrabile	API	Requisiti	Link al repository GitHub
SI	API A PAGAMENTO, con versione free limitata	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• requests==2.26.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/intezer-sandbox

IPinfo

Con questo connettore si possono individuare le posizioni degli utenti, personalizzare le loro esperienze, prevenire le frodi, garantire la conformità e molto altro ancora. Veloce, preciso e scelto da oltre 300.000 aziende e sviluppatori dal 2013

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	L'utilizzo gratuito della nostra API è limitato a 50.000 richieste API al mese.	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycountry==20.7.3• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/ipinfo

Ivre

IVRE è un framework di riconoscione di rete open source, che semplifica la creazione di alternative completamente controllate e self-hosted a servizi come Shodan, ZoomEye, Censys (scansioni di rete estese), Greynoise (monitoraggio degli scanner) e/o PassiveDNS. Il connettore crea relazioni tra osservabili e aggiunge nuovi osservabili.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• pycti == 5.0.3• https://github.com/ivre/ivre• PyYAML	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/ivre

Malbeacon

Questo è un connettore di arricchimento che utilizza l'API Malbeacon per aggiungere informazioni sulle reti di origine degli aggressori. MalBeacon impianta beacon tramite il traffico di check-in dei bot malware. Gli avversari che conducono campagne nefaste in natura amministrando questi pannelli malware C2 ora possono essere monitorati. MalBeacon è uno strumento per i buoni che fornisce informazioni aggiuntive sull'attribuzione degli attacchi.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pydantic==1.7.3• pycti == 5.0.3• urllib3==1.26.5	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/malbeacon

Shodan

È un motore di ricerca che permette di trovare i dispositivi collegati alla rete Internet amministrabili da remoto. Uno strumento che aiuta a capire quant'è importante mettere in sicurezza la rete locale. Entro 5 minuti dall'utilizzo di Shodan Monitor vedrai cosa hai attualmente connesso a Internet all'interno della tua rete e sarai configurato con notifiche in tempo reale quando si presenta qualcosa di imprevisto.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
NO	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• shodan==1.25.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/shodan

Unpac-me

UNPACME è un servizio di spacchettamento automatico di malware. Questi vengono analizzati utilizzando una serie di processi di disimballaggio personalizzati gestiti da OpenAnalysis. Questi processi estraggono tutti i payload crittografati o compressi e restituiscono un set univoco di payload all'utente. In breve, UNPACME automatizza il primo passaggio nel processo di analisi del malware. È attualmente operativo come beta pubblica.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	Versione Beta OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/unpac-me

VirusTotal

Permette l'analisi gratuita di files e/o URLs per scovarne virus o malwares all'interno. Utilizza più di 70 software di [antivirus](#) tra cui Kaspersky, Avira, BitDefender, AVG, ESET, G-Data, Comodo, Malwarebytes e McAfee. Il 7 settembre 2012 è stato annunciato l'acquisto di VirusTotal da parte di [Google](#). È possibile cercare, nel set di dati di VirusTotal, campioni di malware, URL, domini e indirizzi IP in base a proprietà binarie, verdetti di rilevamento antivirus, funzionalità statiche, modelli di comportamento come la comunicazione con host o indirizzi IP specifici, metadati di invio e molte altre nozioni. È possibile individuare i file simili a quello sospettato (oggetto di studio) ed i campioni corrispondenti ai criteri di ricerca possono essere scaricati per ulteriori studi.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	L'API pubblica è limitata a 500 richieste al giorno e una velocità di 4 richieste al minuto. L'API pubblica non deve essere utilizzata in prodotti o servizi commerciali.	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• stix2==2.1.0• plyara~=2.1.1• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-enrichment/virustotal

File import

ImportFileStix

Questo connettore è in grado di importare file JSON/XML contenenti dati STIX1 o STIX2.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• maec==4.1.0.17• stix2-elevator==4.0.1• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-import-file/import-file-stix

ImportReport (PDF)

Questo connettore consente alle organizzazioni di fornire informazioni dal report a OpenCTI.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 4.5.1• L'estensione del file caricato nella piattaforma deve essere .json affinché il connettore possa gestirla.• urllib3==1.26.5• pycti == 5.0.3• beautifulsoup4== 4.9.3• pdfminer.six==20201018• stix==1.2.0.11• pydantic==1.8.2• ioc-finder==6.0.1• dateparser==1.0.0	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-export-file/export-file-stix

File export

ExportFileCSV

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-export-file/export-file-csv

ExportFileSTIX

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-export-file/export-file-stix

ExportFileTXT

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.1.0• pycti == 5.0.3	https://github.com/OpenCTI-Platform/connectors/tree/master/internal-export-file/export-file-txt

Third party modules & plug-in

Cortex

Cortex cerca di risolvere un problema comune: come analizzare gli osservabili che sono stati raccolti, interrogando un singolo strumento anziché diversi?

Cortex, un software open source e gratuito, è stato creato da TheHive Project proprio per questo scopo. Gli osservabili, come indirizzi IP ed e-mail, URL, nomi di dominio, file o hash, possono essere analizzati uno per uno o in modalità bulk utilizzando un'interfaccia Web. Gli analisti possono anche automatizzare queste operazioni grazie all'API Cortex REST.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• six>=1.14.0• pycti• cortexutils	https://github.com/TheHive-Project/Cortex-Analyzers/tree/master/analyzers/OpenCTI

Maltego

Maltego è un tool sviluppato dalla società Paterva, che offre la possibilità OSINT (Open Source INTelligence) cioè di raccogliere informazioni tramite la consultazione di dati pubblicamente accessibili e raggrupparle, in formato grafico. Tramite questo strumento si è in grado di raccogliere informazioni da:

- Siti web
- Comunicazioni web (social network, wiki, blog, ...)
- Dati pubblici (conferenze stampa, rapporti dei governi, dati demografici, ...)
- Osservazioni dirette (dati geolocalizzati, conversazioni radio, foto satellitari, ...)
- Professionisti ed accademici (simposi, conferenze, pubblicazioni scientifiche, associazioni professionali, ...)

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN per usi non commerciali	<ul style="list-style-type: none">• OpenCTI Platform >= 5.0.0• Python >= 3.6• maltego-trx==1.3.8• stix2==2.1.0• six>=1.4.0• markdown==3.3.4• pycti>=5.0.1• maltego-stix2>=2.1.1	https://github.com/amrcossi/opencti-maltego

Connettori custom

Anyrun

È una malware sandbox online, per la ricerca dinamica e statica della maggior parte dei tipi di malware. Può analizzare diversi tipi di contenuto come file java, documenti office, file PDF, script, e-mail ed archivi compressi in formati zip, rar, etc.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• pycti == 5.1.3• web-socket.client=0.56.0	Non presente

Trendmicro

TrendMicro è stato sviluppato come connettore di external import. Nello specifico TrendMicro importa report e osservabili.

Integrabile	API pubblica	Requisiti	Link al repository GitHub
SI	OPEN	<ul style="list-style-type: none">• pycti == 5.0.3• feedrss == 6.0.8	Non presente

CONFIGURAZIONE DEI CONNETTORI

I connettori possono essere configurati ed eseguiti in due modi distinti:

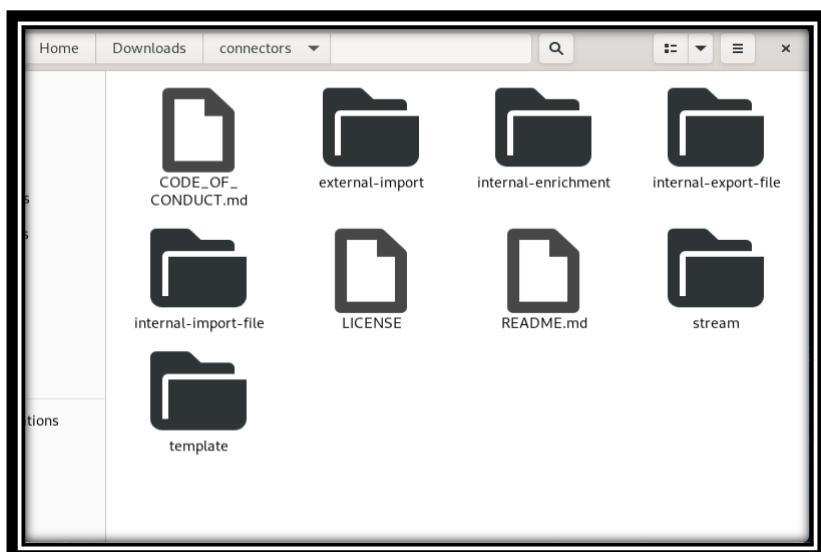
- Manualmente
- Tramite container docker

Configurazione Manuale

Dopo l'avvio della VM, per la configurazione manuale occorre installare delle dipendenze coi seguenti comandi:

1. NodeJS: *apt install nodejs npm python3 python3-pip*
2. Redis-Server: *apt install redis-server*
3. RabbitMQ-Server: *apt install rabbitmq-server*
4. RabbitMQ Management Plugin: *rabbitmq-plugins enable rabbitmq_management*

Successivamente bisogna scaricare il repository GitHub con tutti i connettori, ripartiti per categorie, tramite il comando *git clone <https://github.com/OpenCTI-Platform/connectors>*.



Directory dei connettori dopo il comando git clone

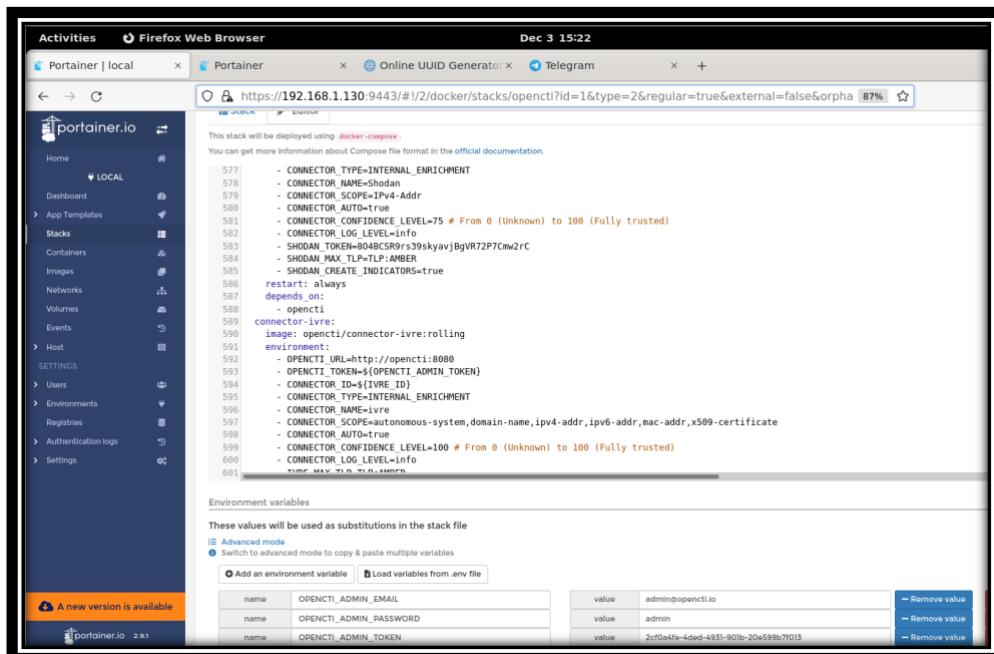
A questo punto, per ogni connettore è necessario seguire i seguenti passaggi:

1. Apertura della directory con i file requirements.txt, config.yml.sample ed eseguibile python
2. Da terminale, esecuzione del comando `pip3 install -r requirements.txt` per scaricare le dipendenze dell'eseguibile python
3. Configurazione del file config.yml.sample, con l'eventuale inserimento dell'api key per abilitare il connettore
4. Creazione del file .yml con il comando `cp config.yml.sample config.yml`
5. Esecuzione del comando `python3 <nome dell'eseguibile>.py` per avviare il connettore e mandarlo in stato di running

Configurazione Tramite Container Docker

Per la gestione dei connettori tramite container docker, invece, si può utilizzare Portainer.io, una piattaforma dalla quale è possibile configurare tutti i connettori all'interno di un unico file, denominato docker-compose.yml, accessibile dalla piattaforma via browser.

In questo caso, dopo l'avvio della VM, bisogna connettersi all'url `https://IP_OPENCTI:9443` e accedere al suddetto file .yml.



File docker-compose.yml di Portainer.io

Configurazione Tramite Container Docker VS Manuale

Anche se, teoricamente, le due configurazioni dovrebbero essere equivalenti, quella manuale presenta alcuni svantaggi:

- Occorre scaricare numerose dipendenze e prerequisiti
- Per eseguire ogni connettore è necessario un terminale da cui lanciare il comando di avvio. Di conseguenza, occorrerebbe avviarli in modalità detached, oppure scrivere uno script python che si occupi ogni volta di avviarli tutti
- Alcuni connettori, se eseguiti manualmente, non funzionano in modo propriamente corretto

Di conseguenza, la configurazione tramite docker risulta essere l'approccio migliore, nonché quello scelto.

Registered connectors					
#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	MODIFIED
1	AMITI	Data import	NOT APPLICAB.	0	Dec 1, 2021, 6:13:54 PM
2	Abuse.ch URLhaus	Data import	NOT APPLICAB.	0	Dec 1, 2021, 6:13:20 PM
3	AbuseIPDB	Enrichment	AUTOMATIC	0	Nov 27, 2021, 3:13:27 PM
4	AlienVault	Data import	NOT APPLICAB.	0	Dec 1, 2021, 6:13:22 PM
5	BackupFiles	Streaming	NOT APPLICAB.	0	Nov 28, 2021, 2:53:36 AM
6	Common Vulnerabilities and Exposures	Data import	NOT APPLICAB.	0	Dec 1, 2021, 6:13:20 PM
7	Cryptolaemus	Data import	NOT APPLICAB.	0	Nov 30, 2021, 10:10:00 PM
8	CyberThreatCoalition	Data import	NOT APPLICAB.	0	Nov 28, 2021, 2:09:46 AM
9	ExportFileCsv	Files export	NOT APPLICAB.	0	Nov 28, 2021, 2:40:01 AM
10	ExportFileCsv	Files export	NOT APPLICAB.	0	Dec 1, 2021, 7:53:00 PM
11	ExportFileStix	Files export	NOT APPLICAB.	0	Nov 28, 2021, 2:42:28 AM
12	ExportFileStix2	Files export	NOT APPLICAB.	0	Dec 1, 2021, 7:53:01 PM
13	ExportFileTxt	Files export	NOT APPLICAB.	0	Nov 28, 2021, 2:46:10 AM
14	GreyNoise	Enrichment	AUTOMATIC	0	Nov 27, 2021, 3:14:30 PM
15	Hatching Triage Sandbox	Enrichment	MANUAL	0	Nov 30, 2021, 5:38:24 PM

Sezione “connettori” di OpenCTI Dopo la configurazione

Workers

I workers sono processi python autonomi che effettuano delle query di scrittura asincrona. Per aumentare il volume di dati importati dai connettori sarebbe opportuno aumentare il numero di workers. In questo modo si hanno più processi che possono occuparsi del download dei dati dai connettori e del relativo salvataggio nella base di dati di OpenCTI.

La modifica del numero di workers può essere effettuata direttamente dallo stack modificando il campo replicas.

Stack details 

[Stacks](#) > opencti

This stack will be deployed using `docker-compose`.

You can get more information about Compose file format in the [official documentation](#).

```
//      - elasticsearch
78      - minio
79      - rabbitmq
80      restart: always
81 worker:
82   image: opencti/worker:5.0.3
83   environment:
84     - OPENCTI_URL=http://opencti:8080
85     - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
86     - WORKER_LOG_LEVEL=info
87   depends_on:
88     - opencti
89   deploy:
90     mode: replicated
91     replicas: 10
92     restart: always
93 connector-history:
94   image: opencti/connector-history:5.0.3
95   environment:
96     - OPENCTI_URL=http://opencti:8080
97     - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
98     - CONNECTOR_ID=${CONNECTOR_HISTORY_ID} # Valid UUIDv4
```

Dopo la modifica e dopo aver eseguito l'update dello stack, il numero di workers sarà modificato anche nella dashboard.

The screenshot shows the OpenCTI platform interface. On the left, there's a sidebar with navigation links: Dashboard, Activities, Analysis, Events, Observations, Knowledge, Threats, Arsenal, and Entities. The 'Data' link is currently selected. At the top, there are tabs for Entities, Background tasks, Connectors (which is the active tab), Synchronization, Data sharing, and TAXII collections. A search bar is also at the top right. The main area has a dark background with light-colored text. It displays 'Workers statistics' with values: 10 CONNECTED WORKERS, 975.58K QUEUED BUNDLES, 9.4/s BUNDLES PROCESSED, 543.8/s READ OPERATIONS, 7.1M/s WRITE OPERATIONS, and 3.25M TOTAL NUMBER OF DOCUMENTS. Below this, there's a section titled 'Registered connectors' with a table:

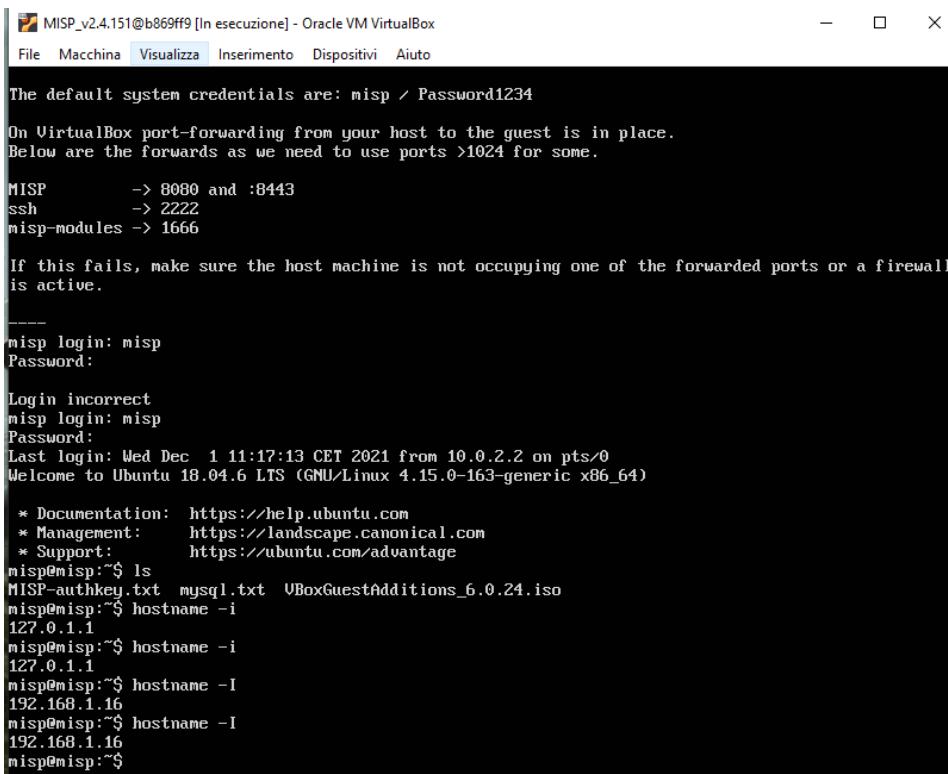
#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	MODIFIED
1	AMITI	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:06 PM
2	Abuse.ch URLhaus	Data import	NOT APPLICAB.	70.29K	Dec 13, 2021, 5:01:39 PM
3	AbusePOB	Enrichment	AUTOMATIC	0	Dec 13, 2021, 5:02:05 PM
4	AlienVault	Data import	NOT APPLICAB.	869.58K	Dec 13, 2021, 5:01:35 PM
5	BackupFiles	Streaming	NOT APPLICAB.	0	Dec 13, 2021, 5:02:05 PM
6	CAPE	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:09 PM
7	Common Vulnerabilities and Exposures	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:07 PM
8	Cryptominers	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:06 PM
9	CyberThreatCoalition	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:03 PM
10	Cybercrime-Tracker	Data import	NOT APPLICAB.	0	Dec 13, 2021, 5:02:06 PM
11	ExportFileCsv	Files export	NOT APPLICAB.	0	Dec 13, 2021, 5:02:09 PM
12	ExportFileTxt2	Files export	NOT APPLICAB.	0	Dec 13, 2021, 5:02:07 PM
13	ExportFileTxt	Files export	NOT APPLICAB.	0	Dec 13, 2021, 5:02:07 PM
14	Hatching Triage Sandbox	Enrichment	MANUAL	0	Dec 13, 2021, 5:02:07 PM
15	AlienVault	Streaming	NOT APPLICAB.	0	Dec 13, 2021, 5:02:03 PM

Configurazione di MISP ed abilitazione dei feed

MISP è una piattaforma di intelligence che consente la condivisione, l'archiviazione e la correlazione di indicatori di compromissione, intelligence sulle minacce, informazioni sulle frodi finanziarie, informazioni sulle vulnerabilità o persino informazioni sull'antiterrorismo.

Per abilitare il connettore MISP bisogna:

- Scaricare e importare la macchina virtuale di MISP (<https://vm.misp-project.org/>).
- Avviare la macchina virtuale e loggarsi (admin: misp e password: misp)



The default system credentials are: misp / Password1234
On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.
MISP -> 8080 and :8443
ssh -> 2222
misp-modules -> 1666
If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall is active.

misp login: misp
Password:
Login incorrect
misp login: misp
Password:
Last login: Wed Dec 1 11:17:13 CET 2021 from 10.0.2.2 on pts/0
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-163-generic x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
misp@misp:~\$ ls
MISP-authkey.txt mysql.txt VBoxGuestAdditions_6.0.24.iso
misp@misp:~\$ hostname -i
127.0.1.1
misp@misp:~\$ hostname -i
127.0.1.1
misp@misp:~\$ hostname -I
192.168.1.16
misp@misp:~\$ hostname -I
192.168.1.16
misp@misp:~\$

- Prelevare l'IP della macchina
- Connettersi al servizio sulla porta 80 (<https://192.168.1.16>)
- Autenticarsi: al primo avvio l'username sarà admin@admin.test e la password admin. Successivamente sarà possibile effettuare il cambio password.
- Generare un'api key: Selezionare la sezione Global Actions e poi cliccare su My Profile. In figura viene mostrata la sezione che contiene le informazioni relative all'utente e la lista delle api key create.

User admin@admin.test

ID	1
Email	admin@admin.test
Organisation	ORIONNAME
Role	admin
Event alert enabled	No
Contact alert enabled	No
Invited By	N/A
NIDS Start SID	4000000
PGP Key	N/A
Created	N/A

[Download user profile for data portability](#)

Auth keys

#	User	Auth Key	Expiration	Last used	Comment	Actions
1	admin@admin.test	spzXXXXXXXXXX	Indefinite	Never	Initial auto-generated key	Edit Delete
2	admin@admin.test	6DZXXXXXXXXXX	Indefinite	Never	Map	Edit Delete

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2.

[« previous](#) [next »](#)

Events

Add auth key

Auth keys are used for API access. A user can have more than one authkey, so if you would like to use separate keys per tool that queries MISP, add additional keys. Use the comment field to make identifying your keys easier.

User

admin@admin.test

Comment

Allowed IPs

Expiration (keep empty for indefinite)

YYYY-MM-DD

Read only (it will be not possible to do any change operation with this token)

[Submit](#) [Cancel](#)

Definita la policy per l'api key è possibile confermarne la creazione cliccando su submit.

- Aggiungere feed: i feed sono documenti (txt, JSON, csv) che contengono informazioni relative a minacce, indicatori di compromissione, etc... Per aggiungere i feed bisogna loggarsi sulla piattaforma MISP, cliccare nella sezione Sync Action e poi su list feed.

L’interfaccia utente mostrerà tutti i feed caricati.

The screenshot shows the 'Feeds' section of a web application. At the top, there are several navigation links: Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. Below these, a sidebar on the left contains links for 'List Feeds', 'Search Feed Caches', 'Add Feed', 'Import Feeds from JSON', 'Feed overlap analysis matrix', and 'Export Feed settings'. The main area is titled 'Feeds' and contains a sub-header: 'Generate feed lookup caches or fetch feed data (enabled feeds only)'. There are four buttons at the top right: 'Load default feed metadata' (disabled), 'Cache all feeds', 'Cache freeText/CSV feeds', 'Cache MISP feeds', and a prominent blue button 'Fetch and store all feed data'. Below these buttons is a pagination bar with links for '< previous', '1', '2', '3', 'next >', and 'last >'. A table follows, with columns: 'Default feeds', 'Custom feeds', 'All feeds' (which is selected and highlighted in blue), and 'Enabled feeds'. The table has a header row with columns: 'ID', 'Enabled', 'Caching', 'Name', 'Format', 'Provider', 'Org', 'Source', and 'URL'. Below this header are nine rows of data, each representing a feed. The feeds listed are:

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL
1	✓	✗	CIRCL OSINT Feed	misp	CIRCL	network	https://www.circl.lu/doc/misp/feed/osint	
2	✓	✗	The Botvrij.eu Data	misp	Botvrij.eu	network	https://www.botvrij.eu/data/feed-o	
3	✓	✗	CIRCL OSINT FEED	misp	CIRCL	network	https://www.circl.lu/doc/misp/feed/osint/	
4	✓	✗	Botvrij	misp	Botvrij	network	https://www.botvrij.eu/data/feed-o	
5	✓	✗	blockrules of rules	misp	blockrules of rules	network	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	
6	✓	✗	Tor exit nodes	misp	Tor exit nodes	network	https://www.dan.me.uk/torlist/?exitnodes	
7	✓	✗	Tor ALL nodes	misp	Tor ALL nodes	network	https://www.dan.me.uk/torlist/	
8	✓	✗	cybercrime-tracker.net	misp	cybercrime-tracker.net	network	https://cybercrime-tracker.net/all_c	
9	✓	✗	Phishtank online valid phishing	misp	Phishtank online valid phishing	network	https://data.phishtank.com/valid-phishing	

Bisogna poi cliccare su “Add Feed” e specificare almeno il nome, il provider, la sorgente, l’url e la sorgente dei dati.

The screenshot shows the 'Add MISP Feed' form. On the left, a sidebar lists 'List Feeds', 'Search Feed Caches', 'Add Feed' (which is selected and highlighted in blue), 'Import Feeds from JSON', 'Feed overlap analysis matrix', and 'Export Feed settings'. The main form area has a title 'Add MISP Feed'. It includes fields for 'Name' (with placeholder 'Feed name'), 'Provider' (with placeholder 'Name of the content provider'), 'Input Source' (set to 'Network'), 'URL' (with placeholder 'URL of the feed'), 'Source Format' (set to 'MISP Feed'), and a text area for 'Any headers to be passed with requests (for example: Authorization)' containing the placeholder 'Line break separated list of headers in the "headername: value" format'. Below these are sections for 'Distribution' (set to 'All communities') and 'Default Tag' (set to 'None'). At the bottom, there is a 'Filter rules:' section with a 'Modify' button, and a large blue 'Submit' button.

Successivamente sono stati sviluppati dagli scenari di test per testare il funzionamento della piattaforma MISP e per testare l’interazione tra MISP e OpenCTI.

Nel seguente scenario di test sono stati aggiungi dei feed alla piattaforma MISP, e poi, è stato verificato se effettivamente le informazioni venivano importate e mostrate nella dashboard.

Feed aggiunti:

- CIRCL OSINT Feed
- The Botvrij.eu Data
- Tor exit nodes
- Home.nuug.no
- emergingngthreats

Dashboard:

The screenshot shows the MISP dashboard at the URL <https://192.168.1.16/events/index/published:1?laststamp=1639320666>. The interface includes a top navigation bar with links for Home, Event Actions, Dashboard, Galleries, Input Filters, Global Actions, Sync Actions, Administration, Logs, and API. On the left, there are sidebar sections for 'Last Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'Export Automation', and 'Import'. The main content area displays a list of events. One event is expanded to show its details, including its creation date (2021-11-16), creator (admin@admin.test), and tags (circincident classification="malware", circincident classification="phishing"). The event also lists various attack patterns and their sub-patterns, such as 'Attack Pattern Q' and 'File and Directory Discovery - T1082 Q'. Other events listed include 'ORNAME' (ORNAME) and 'Attack Pattern Q' (Attack Pattern Q). The bottom right corner of the dashboard shows the date (2021-09-14), the number of events (18), and the number of alerts (4).

Come si può osservare dalla precedente figura, le informazioni vengono correttamente integrate e mostrate nella dashboard di MISP.

Il seguente scenario di test prevede la verifica dell’interazione tra OPENCTI e MISP. Nello specifico è stato verificato se nella dashboard di OPENCTI venivano correttamente importate le informazioni proveniente dalla piattaforma MISP.

Come si può osservare in figura l'api key generata per consentire l'interazione tra MISP e OpenCTI è stata utilizzata.

#	User	Auth Key	Expiration	Last used	Comment	Allowed IPs	Actions
1	admin@admin.test	5847*****10f9f	Indefinite	Never	Initial auto-generated key	<input type="text"/>	
2	admin@admin.test	692D*****4c10f	Indefinite	Never	Misp	<input type="text"/>	
3	admin@admin.test	8704*****q15m	Indefinite	2021-12-14 14:37:29		<input type="text"/>	

Inoltre, il connettore è stato correttamente importato nella lista dei connettori di OpenCTI.

Connector	Type	Last Used	Created
Cryptolaeus	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:39 AM
CyberThreatCoalition	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:46 AM
Cybercrime-Tracker	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:39 AM
ExportFileCsv	Files export	NOT APPLICAB.	Dec 15, 2021, 7:49:46 AM
ExportFileStix	Files export	NOT APPLICAB.	Dec 15, 2021, 7:49:36 AM
ExportFileTxt	Files export	NOT APPLICAB.	Dec 15, 2021, 7:49:41 AM
Hatching Triage Sandbox	Enrichment	MANUAL	Dec 15, 2021, 7:49:46 AM
History	Streaming	NOT APPLICAB.	Dec 15, 2021, 7:49:40 AM
Hybrid Analysis (Sandbox Windows 10 64bit)	Enrichment	AUTOMATIC	Dec 15, 2021, 7:49:39 AM
Hygiene	Enrichment	AUTOMATIC	Dec 15, 2021, 7:49:40 AM
ImportExternalReference	Enrichment	MANUAL	Dec 15, 2021, 7:49:39 AM
ImportFileStix	Files import	MANUAL	Dec 15, 2021, 7:49:45 AM
ImportReport	Files import	MANUAL	Dec 15, 2021, 7:49:46 AM
IntezerSandbox	Enrichment	MANUAL	Dec 15, 2021, 7:49:39 AM
IpInfo	Enrichment	AUTOMATIC	Dec 15, 2021, 7:49:39 AM
MISP	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:46 AM
MITRE ATT&CK	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:45 AM
Malpedia	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:39 AM
OpenCTI	Data import	NOT APPLICAB.	Dec 15, 2021, 7:49:45 AM
OpenCTI Elastic Connector	Streaming	NOT APPLICAB.	Dec 15, 2021, 7:50:06 AM

Le informazioni importate dal connettore sono le seguenti:

Entity Type	Count
Vulnerability	4 entities
Indicator	5 entities
Attack Pattern	1 entity

Configurazione, sviluppo e testing del connettore Anyrun

Anyrun è stato sviluppato come connettore di Enrichment. Nello specifico, Anyrun va ad arricchire la descrizione delle famiglie di malware presenti nella piattaforma OpenCTI.

Siccome non sono presenti delle Api online che consentono di ottenere le informazioni di anyrun è stato integrato il client di PyPI([anyrun · PyPI](#)).

Il client apre una websocket verso anyrun:

```
def connect(self):
    url = "wss://app.any.run/sockjs/1/test/websocket".format(
        id=AnyRunClient.generate_id(),
        token=AnyRunClient.generate_token()
    )

    print('Trying to connect to ' + url)
    self._con = websocket.WebSocketApp(
        url=url,
        on_message=self.on_message,
        on_error=self.on_error,
        on_close=self.on_close
    )
    self._con.on_open = self._init_connection
```

Nel metodo `init_connection` vengono specificate le tipologie di informazioni che è possibile ottenere:

```
def _init_connection(self):
    self.send_message({"msg": "connect", "version": "1", "support": ["1", "pre2", "pre1"]})
    self.send_message({"msg": "method", "method": "host", "params": [], "id": "1"})
    self.send_message({"msg": "method", "method": "getPrefix", "params": [], "id": "2"})

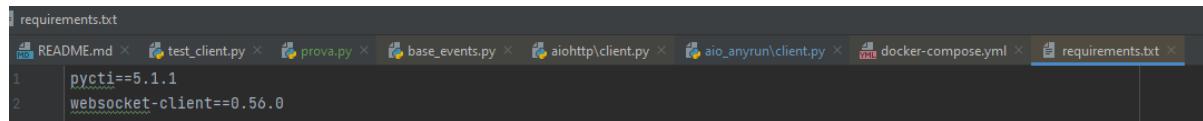
    self.subscribe('statisticsDayTags')
```

Compreso il funzionamento del client si è passati alla fase di configurazione del connettore e l'individuazione dei requisiti necessari all'installazione.

Il seguente file docker-compose.yml contiene la configurazione del connettore:

```
version: '3'
services:
  connector-anyrun:
    image: pietrovitagliano/anyrun:0.320
    environment:
      - OPENTI_URL=http://openti:8080
      - OPENTI_TOKEN=${OPENTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_ANYRUN_ID}
      - CONNECTOR_TYPE=INTERNAL_ENRICHMENT
      - CONNECTOR_NAME=Anyrun
      - CONNECTOR_SCOPE=StixFile,Artifact,Url,Domain,X-OpenCTI-Hostname,attack-pattern,intrusion-set,malware,report,attack-info # MIME type or Stix Object
      - CONNECTOR_AUTO=true # Enable/disable auto-enrichment of observables
      - CONNECTOR_CONFIDENCE_LEVEL=100 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
      - openti
```

I requisiti di installazione sono contenuti nel file requirements.txt:



```
requirements.txt
1 pycti==5.1.1
2 websocket-client==0.56.0
```

La seconda fase è stata lo sviluppo del connettore.

I passaggi salienti dello sviluppo sono:

- Caricamento della configurazione del connettore (contenuta nel file yml):



```
class AnyRun:
    def __init__(self):
        # Instantiate the connector helper from config
        config_file_path = os.path.dirname(os.path.abspath(__file__)) + "/config.yml"

        config = (
            yaml.load(open(config_file_path), Loader=yaml.FullLoader)
            if os.path.isfile(config_file_path)
            else {}
        )

        self.helper = OpenCTIConnectorHelper(config)

        self.descriptionEnrichment = "This malware family has been executed on an AnyRun sandbox"
        self.clientMalwareInfo = []

        self.identity = self.helper.api.identity.create(
            type="Organization",
            name="AnyRun",
            description="Internal Enrichment Connector",
        )["standard_id"]
```

- Avvio del client:

```

    def startClient(self):
        self.client = AnyRunClient(
            on_message_cb=self.callback,
            enable_trace=False
        )

        self.client.connect()
        self.client.run_forever()
    
```

- Ricerca della famiglia dei malware e arricchimento: l'arricchimento avviene invocando il metodo _process_message, ogni volta che nuovi dati arrivano su OpenCTI (programmazione a eventi)

```

def _process_message(self, data):
    entity_id = data["entity_id"]
    entity = self.helper.api.stix_domain_object.read(id=entity_id)

    if(entity is None):
        raise ValueError("Entity not found")
    else:
        self.helper.log_info("Stix Domain Object detected. Check if it's malware")
        if(entity["entity_type"].lower() == "malware"):
            self.helper.log_info("Malware detected. Check if already on the platform")
            while(len(self.clientMalwareInfo) == 0):
                time.sleep(5)

            for dict in self.clientMalwareInfo:
                if (dict["fields"]["tag"].lower() == entity["name"].lower() or dict["fields"]["tag"].lower() in (malwareType.lower() for malwareType in entity["malware_types"])):
                    self.helper.log_info("Malware info already are on OpenCTI")

                    if (self.descriptionEnrichment in entity["description"]):
                        return "Malware already enriched"
                    else:
                        newDescription = entity["description"] + "\n" + self.descriptionEnrichment
                        self.helper.api.stix_domain_object.update_field(
                            id=entity["id"],
                            input={"key": "description", "value": newDescription},
                        )
    
```

- Creazione dell'immagine Docker:

docker image build -t pietrovitagliano/anyrun:0.41

- Aggiornamento dello stack

```

connector-anyrun:
    image: pietrovitagliano/anyrun:0.41
    environment:
        - OPENTI_URL=http://opentci:8080
        - OPENTI_TOKEN=${OPENTI_ADMIN_TOKEN}
        - CONNECTOR_ID=${CONNECTOR_ANYRUN_ID}
        - CONNECTOR_TYPE=INTERNAL_ENRICHMENT
        - CONNECTOR_NAME=Anyrun
        - CONNECTOR_SCOPE=Stixfile,Artifact,Domain,X-OpenCTI-Hostname,attack-pattern,intrusion-set,malware,report,attack-info # MIME type or Stix Object
        - CONNECTOR_AUTO=true # Enable/disable auto-enrichment of observables
        - CONNECTOR_CONFIDENCE_LEVEL=100 # From 0 (Unknown) to 100 (Fully trusted)
        - CONNECTOR_LOG_LEVEL=info
    restart: always
    depends_on:
        - opentci
    
```

La terza fase è stata il testing del connettore Anyrun.

Nel seguente scenario di test si verifica che:

- Anyrun sia stato correttamente importato nella lista dei connettori

The screenshot shows the OPENCTI platform's dashboard. At the top, there are several performance metrics: 10 CONNECTED WORKERS, 106.32K QUEUED BUNDLES, 2.4/s BUNDLES PROCESSED, 421.6/s READ OPERATIONS, 492/s WRITE OPERATIONS, and 5.19M TOTAL NUMBER OF DOCUMENTS. Below these metrics is a table titled "Registered connectors". The table has columns for #, NAME, TYPE, AUTOMATIC TRIGGER, MESSAGES, and MODIFIED. The connectors listed are: AMITI, Abusech URI haus, AbuselPOB, AlienVault, Anyrun, BackupFiles, CAPE, Common Vulnerabilities and Exposures, Cryptolaeus, CyberThreatCoalition, and Cybercrime-Tracker. Each connector entry includes a small green star icon and a preview button.

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	MODIFIED
1	AMITI	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:35 PM
2	Abusech URI haus	Data import	NOT APPLICAB.	88.19K	Dec 19, 2021, 12:03:37 PM
3	AbuselPOB	Enrichment	AUTOMATIC	8	Dec 19, 2021, 12:03:35 PM
4	AlienVault	Data import	NOT APPLICAB.	6.11K	Dec 19, 2021, 12:03:35 PM
5	Anyrun	Enrichment	AUTOMATIC	55	Dec 19, 2021, 12:03:20 PM
6	BackupFiles	Streaming	NOT APPLICAB.	0	Dec 19, 2021, 12:03:35 PM
7	CAPE	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:37 PM
8	Common Vulnerabilities and Exposures	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:16 PM
9	Cryptolaeus	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:18 PM
10	CyberThreatCoalition	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:14 PM
11	Cybercrime-Tracker	Data import	NOT APPLICAB.	0	Dec 19, 2021, 12:03:14 PM

- Anyrun abbia arricchito correttamente le informazioni: come possiamo osservare in figura, anyrun va ad arricchire la descrizione specificando che per quella famiglia di malware è stato eseguito un task nel sandbox di anyrun.

The screenshot shows the entity details page for a malware sample named "ADWARE". The left sidebar shows the navigation menu. The main area is divided into two sections: "BASIC INFORMATION" and "DETAILS".
In the "BASIC INFORMATION" section:

- Standard STIX ID: malware--b6d77822-2e02-54f0-abbb-19d7b6e25c9
- Other STIX IDs: (empty)
- Marking:
 - Author: -
 - Distribution of opinions: 5 points (strongly-agree, agree, neutral, disagree, strongly-disagree)
 - Confidence level: LOW
- Creation date (in this platform): December 20, 2021, 4:31:11 PM
- Creator: ADMIN
- Modification date: December 20, 2021, 6:00:00 PM

In the "DETAILS" section:

- la family: NOT APPLICAB.
- Description: Descrizione di prova
This malware family has been executed on an Anyrun sandbox.
- Architecture execution env: Unknown
- Kill chain phases: Kill chain phases
- Implementation languages: Unknown
- Capabilities: Unknown

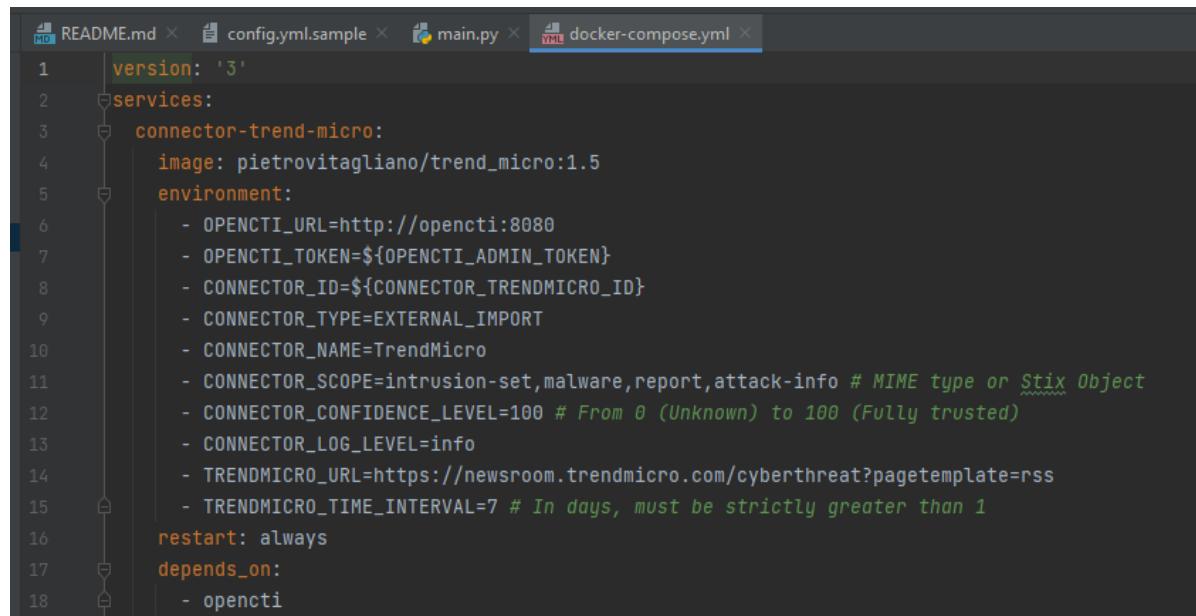
At the bottom, there are two sections: "LATEST CREATED RELATIONSHIPS" and "LATEST REPORTS ABOUT THIS ENTITY", both of which state: "No entities of this type has been found."

Non è stato possibile arricchire con ulteriori informazioni perché è necessario acquistare una licenza. In conclusione, si può affermare che il test ha avuto esito positivo.

Configurazione, sviluppo e testing del connettore Trend Micro

Trend Micro è stato sviluppato come connettore di external import. Nello specifico Trend Micro importa report e osservabili. La prima fase è stata la configurazione del connettore e l'individuazione dei requisiti necessari all'installazione del connettore.

Il seguente file docker-compose.yml contiene la configurazione del connettore:

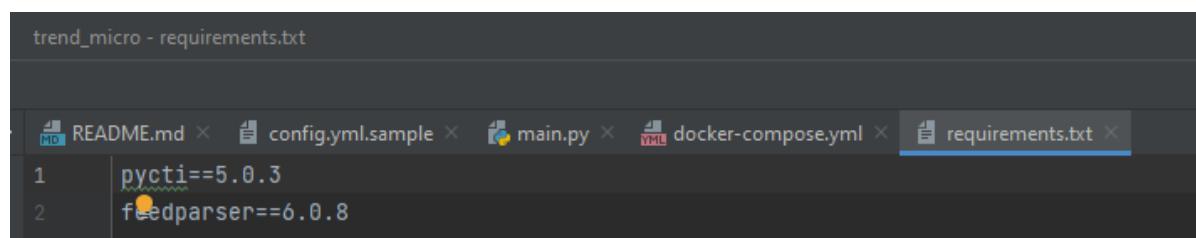


```
version: '3'
services:
  connector-trend-micro:
    image: pietrovitagliano/trend_micro:1.5
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
      - CONNECTOR_ID=${CONNECTOR_TRENDMICRO_ID}
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - CONNECTOR_NAME=TrendMicro
      - CONNECTOR_SCOPE=intrusion-set,malware,report,attack-info # MIME type or Stix Object
      - CONNECTOR_CONFIDENCE_LEVEL=100 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_LOG_LEVEL=info
      - TRENDMICRO_URL=https://newsroom.trendmicro.com/cyberthreat?pagetemplate=rss
      - TRENDMICRO_TIME_INTERVAL=7 # In days, must be strictly greater than 1
    restart: always
    depends_on:
      - opencti
```

Come si può osservare in figura, i feed RSS vengono forniti dal seguente url:

<https://newsroom.trendmicro.com/cyberthreat?pagetemplate=rss>

I requisiti di installazione sono contenuti nel file requirements.txt:



```
trend_micro - requirements.txt

pycti==5.0.3
feedparser==0.8
```

La seconda fase è stata lo sviluppo del connettore.

I passaggi salienti dello sviluppo sono:

- Caricamento della configurazione del connettore (contenuta nel file .yml) e connessione all'url di Trend Micro

```

10
11     class TrendMicroConnector:
12         def __init__(self):
13             # Instantiate the connector helper from config
14             config_file_path = os.path.dirname(os.path.abspath(__file__)) + "/config.yml"
15             config = (
16                 yaml.load(open(config_file_path), Loader=yaml.FullLoader)
17                 if os.path.isfile(config_file_path)
18                 else {}
19             )
20
21             self.helper = OpenCTIConnectorHelper(config)
22
23             self.trendmicro_url = get_config_variable(
24                 "TRENDMICRO_URL", ["trendmicro", "trendmicro"], config, False
25             )
26
27             self.time_interval = get_config_variable(
28                 "TRENDMICRO_TIME_INTERVAL", ["trendmicro", "time_interval"], config, True
29             )

```

- Sottomissione del bundle a OpenCTI: il bundle creato racchiude oggetti creati attraverso AttackPattern. Creato il bundle viene inviato a OpenCTI utilizzando la funzione send_stix2_bundle().

```

def parseRssTrendMicroFeedToStix2Bundle(self, rssFeedTrendMicroUrl):
    rss_feed = feedparser.parse(rssFeedTrendMicroUrl)

    objectsList = []
    for entry in rss_feed.entries:
        dateTimeObj = datetime.strptime(entry.published[5: 25], '%d %b %Y %H:%M:%S')

        attack_pattern = AttackPattern(
            id=OpenCTIStix2Utils.generate_random_stix_id("attack-pattern"),
            name=entry.title,
            created=dateTimeObj.strftime("%Y-%m-%dT%H:%M:%S.000Z"),
            created_by_ref=self.identity,
            description=entry.description,
            external_references=[
                {
                    "source_name": entry.title,
                    "url": entry.link
                }
            ]
        )

        objectsList.append(attack_pattern)

    return Bundle(objects=objectsList, allow_custom=True).serialize()

}

# Try to send json data to OpenCTI platform
self.helper.log_info("Sending data to OpenCTI...")
try:
    bundle = self.parseRssTrendMicroFeedToStix2Bundle(rssFeedTrendMicroUrl = self.trendmicro_url)
    print(bundle)

    self.helper.send_stix2_bundle(bundle)

    # Store the current timestamp as a last run
    message = "Connector successfully run, storing last_run as " + str(timestamp)
    self.helper.log_info(message)
    self.helper.set_state({"last_run": timestamp})
    self.helper.api.work.to_processed(work_id, message)
    self.helper.log_info("Last_run stored, next run in: " + str(round(self.get_interval() / 60 / 60 / 24, 2)) + " days")

```

- Creazione dell'immagine Docker:

```
docker image build -t pietrovitagliano/trend_micro:1.52
```

- Aggiornamento dello stack

```
connector-trend-micro:
  image: pietrovitagliano/trend_micro:1.52
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_TRENDMICRO_ID}
    - CONNECTOR_TYPE=EXTERNAL_IMPORT
    - CONNECTOR_NAME=TrendMicro
    - CONNECTOR_SCOPE=attack-pattern,intrusion-set,malware,report,attack-info # MIME type or Stix Object
    - CONNECTOR_CONFIDENCE_LEVEL=100 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
    - TRENDMICRO_URL=https://newsroom.trendmicro.com/cyberthreat?pagetemplate=rss
    - TRENDMICRO_TIME_INTERVAL=7 # In days, must be strictly greater than 1
  restart: always
  depends_on:
    - opencti
```

La terza fase è stata il testing del connettore Trend Micro.

Nel seguente scenario di test si verifica che:

- Trend Micro sia stato correttamente importato nella lista dei connettori

ImportExternalReference	Enrichment	MANUAL	0	Dec 13, 2021, 6:06:55 PM		
ImportFileStix	Files import	MANUAL	0	Dec 13, 2021, 6:06:40 PM		
ImportReport	Files import	MANUAL	0	Dec 13, 2021, 6:06:45 PM		
InterceptorSandbox	Enrichment	MANUAL	0	Dec 13, 2021, 6:06:39 PM		
IpInfo	Enrichment	AUTOMATIC	0	Dec 13, 2021, 6:06:45 PM		
MISP	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:55 PM		
MITRE ATTACK	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:30 PM		
Malpedia	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:40 PM		
OpenCTI	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:30 PM		
OpenCTI Elastic Connector	Streaming	NOT APPLICAB.	0	Dec 13, 2021, 6:06:45 PM		
RISKIQ	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:59 PM		
RestoreFiles	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:55 PM		
SPLUNK	Streaming	NOT APPLICAB.	0	Dec 13, 2021, 6:06:39 PM		
Shodan	Enrichment	AUTOMATIC	6	Dec 13, 2021, 6:06:30 PM		
TrendMicro	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:45 PM		
UnpacMe	Enrichment	MANUAL	0	Dec 13, 2021, 6:06:40 PM		
VX Vault URL list	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:39 PM		
Vulnalls	Data import	NOT APPLICAB.	0	Dec 13, 2021, 6:06:40 PM		

- Trend Micro abbia eseguito dei task

- Trend Micro abbia importato correttamente i dati. Come si può osservare in figura Trend Micro ha importato report, entità e osservabili.

Lista dei reports:

The screenshot shows a search results page for 'Trend micro' in the OpenCTI interface. The left sidebar includes options like Dashboard, Activities, Analysis, Events, Observations, Knowledge (selected), Threats, Arsenal, Entities, Data, and Settings. The main area displays a table of 94 entities under the 'Report' category. Each entry includes a thumbnail icon, the entity name, and a 'No label' button. The entries listed are: MuddyWater TrendMicro June 2018, Trend Micro Emotet Jan 2019, TrendMicro Taidoor, TrendMicro DarkComet Sept 2014, Trend Micro Totbrick Oct 2016, TrendMicro BlackTech June 2017, TrendMicro Msilex Feb 2018, TrendMicro Gamaredon April 2020, TrendMicro TropicTrooper 2015, TrendMicro Tropic Trooper May 2020, TrendMicro Netwalker May 2020, TrendMicro Lazarus Nov 2018, Trend Micro Xbash Sept 2018, TrendMicro Trickbot Feb 2019, TrendMicro PE_URSNIFA2, and TrendMicro Ursnif File Dec 2014.

Osservabili relativi ad IP e URL:

The screenshot shows a detailed view of observables for 'Trend micro' in the OpenCTI interface. The left sidebar is identical to the previous screenshot. The main area is divided into sections: 'Malware' (1 entity, 'Micropia' with a description and a 'malware' button), 'IPv4 address' (8 observable(s) with a list of IP addresses and associated tags like 'self-signed', 'ssl弱', 'email open', 'bad web bot', 'ddos attack', 'email open', 'no label', 'bad web bot', 'code', 'email open', 'phishing', 'malware', 'white list', 'bad web bot', 'http proxy', 'brute force'), 'Domain name' (4 observable(s)), 'URL' (8 observable(s)), and 'Email address' (1 observable(s) with 'microsoft.filter@yandex.com' and tags 'signer', 'malicious', 'phishing').

Struttura di un report Trend Micro:

The screenshot displays the Trend Micro OpenCTI platform interface. On the left, a sidebar navigation includes: Dashboard, Activities, Analysis, Events, Observations, Knowledge (selected), Threats, Arsenal, Entities, Data, and Settings. The main content area shows a report titled "MUDYWATER TRENDMICRO JUNE 2018" with the TLP:WHITE label. The report details include:

- BASIC INFORMATION**:
 - Standard STIX ID: report--52c9655b-2fde-5859-b96a-91ee5efc9de3
 - Other STIX IDs: -
 - Author: TREND MICRO
 - Revoked: NO
 - Labels: +
 - Confidence level: LOW
 - Creation date (in this platform): December 9, 2021, 9:57:03 PM
 - Creator: ADMIN
- ENTITY DETAILS**:
 - Description: Villanueva, M., Co, M. (2018, June 14). Another Potential MuddyWater Campaign uses Powershell-based PIB-Backdoor. Retrieved July 3, 2018.
 - Report types: THREAT REPORT
 - Processing status: NEW
- Distribution of entities**: A donut chart showing distribution percentages:
 - Attack-Pattern (3) 75.00%
 - Intrusion-Set (1) 25.00%
- EXTERNAL REFERENCES**:
 - MuddyWater TrendMicro June 2018: <https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-c...>
- MOST RECENT HISTORY**: A list of recent actions:
 - admin adds Visual Basic in object_refs (Dec 9, 2021, 10:16:55 PM)
 - admin adds relationship--02cfd3b-cf99-4cf6-aed9-cd8e3556dee in object_refs (Dec 9, 2021, 10:16:54 PM)
 - admin adds PowerShell in object_refs (Dec 9, 2021, 10:05:19 PM)

In conclusione, si può affermare che il test ha avuto esito positivo.

Export dei dati

È possibile effettuare l'export delle informazioni (osservabili, minacce, eventi, etc....) nei seguenti formati:

- Txt
- Json
- Csv

Cliccando in alto a destra e selezionando il formato desiderato è possibile procedere con l'export.

TITLE	AUTHOR	LABELS	DATE	STATUS	MARKING
PseudoManuscrypt: a mass-scale spyware attack campaign	AlienVault	glupetra, spyware	Dec 17, 2021	NEW	TLP:WHITE
Serverless InfoStealer delivered in East European Countries	AlienVault	zope, spyware	Dec 17, 2021	NEW	TLP:WHITE
How the Contact Forms campaign tricks people	AlienVault	bazarloader, malware	Dec 16, 2021	NEW	TLP:WHITE
The dirty dozen of Latin America: From Amavaldo to Zumanek	AlienVault	amavaldo, castanero, grandoreiro	Dec 15, 2021	NEW	TLP:WHITE
Espionage Campaign Targets Telecoms Organizations across Middle East an...	AlienVault	chafe, trojan, exploit	Dec 14, 2021	NEW	TLP:WHITE
Owowa: the add-on that turns your OWA into a credential stealer and remote a...	AlienVault	cotura, credential theft, spy	Dec 14, 2021	NEW	TLP:WHITE
New ransomware actor uses password-protected archives to bypass encrypti...	AlienVault	ransomware, planit, ransomware	Nov 19, 2021	NEW	TLP:WHITE
Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange	AlienVault	cve20195591	Nov 18, 2021	NEW	TLP:WHITE
Attackers use domain fronting technique to target Myanmar with Cobalt Strike	AlienVault	cobalt strike, exploit, malware	Nov 17, 2021	NEW	TLP:WHITE
Emotet Returns	AlienVault	botnet, emotet, malware	Nov 16, 2021	NEW	TLP:WHITE
QAKBOT Loader Returns With New Techniques and Tools	AlienVault	cobalt strike, office macro, qakbot	Nov 15, 2021	NEW	TLP:WHITE
[MITRE ATT&CK] Winnti Group (S0044)	The MITRE Corporation	No label	Nov 5, 2021	NEW	TLP:WHITE
[MITRE ATT&CK] Patchwork (S0040)	The MITRE Corporation	No label	Nov 2, 2021	NEW	TLP:WHITE
[MITRE ATT&CK] Kechang (S0004)	The MITRE Corporation	No label	Nov 1, 2021	NEW	TLP:WHITE
[MITRE ATT&CK] B32B05 (S0014)	The MITRE Corporation	No label	Nov 1, 2021	NEW	TLP:WHITE
[MITRE ATT&CK] Monokle (S0407)	The MITRE Corporation	No label	Nov 1, 2021	NEW	TLP:WHITE

Generate an export

application/json

text/plain

text/csv

CANCEL CREATE