

UNIVERSITÀ DEGLI STUDI DEL SANNIO

Corso di Laurea Magistrale in Ingegneria Informatica

Sviluppo Connatori Custom: Urlscanlo, CveTrends, IOCTweet

Docenti del corso:

Prof. Corrado Aaron Visaggio
Dott. Pietro Melillo

Gruppo 'i Serafini':

Compare Carmen
Di Giambattista Serafino
Inglese Jacopo
Zeoli Gabriella

Indice

1. [COSA È UNA PIATTAFORMA DI THREAT INTELLIGENCE](#)
 - 1.1. [Introduzione](#)
 - 1.2. [Definizione di Threat](#)
 - 1.3. [Definizione di Intelligence](#)
2. [PERCHÉ OPENCTI?](#)
 - 2.1. [Architettura OpenCTI](#)
 - 2.2. [STIX2](#)
3. [UBUNTU](#)
4. [OpenCTI](#)
5. [INSTALLAZIONE CONNETTORI](#)
6. [PORAINER](#)
7. [CONNETTORI CUSTOM](#)
 - 7.1. [CVE Trends](#)
 - 7.1.1. [Composizione di un CVE Trend](#)
 - 7.1.2. [Composizione del 'docker-compose' file di CveTrends](#)
 - 7.1.3. [Analisi dei punti salienti del codice](#)
 - 7.2. [Urlscanlo](#)
 - 7.2.1. [Di cosa si compone una ricerca Urlscanlo](#)
 - 7.2.2. [Analisi del 'docker-compose' file](#)
 - 7.2.3. [Analisi dei punti salienti del codice di Urlscanlo](#)
 - 7.3. [IOCTweet](#)
 - 7.3.1. [Composizione del 'docker-compose' file di IOCTweet](#)
 - 7.3.2. [Analisi dei punti salienti del codice di IOCTweet](#)
8. [CASI D'USO](#)
 - 8.1. [CVE Trends](#)
 - 8.2. [Urlscanlo](#)
 - 8.3. [IOCTweet](#)
 - 8.3.1. [Caso d'uso hash file](#)
 - 8.3.2. [Caso d'uso Url](#)

[Esportazione IOC per IOCTweet](#)

[Conclusioni](#)

1. COSA È UNA PIATTAFORMA DI THREAT INTELLIGENCE:

1.1 Introduzione

- a. Definizione: Una Threat Intelligence Platform (TIP) è una soluzione tecnologica che raccoglie, aggrega e organizza i dati di intelligence sulle minacce da più fonti e formati. Un TIP fornisce ai team di sicurezza informazioni sul malware noto e altre minacce, consentendo un'identificazione, un'indagine e una risposta alle minacce efficienti e accurate.

- b. La threat intelligence aiuta le aziende a:

- Rilevare, identificare, convalidare ed indagare su potenziali minacce alla sicurezza, attacchi, attori di minacce dannose e indicatori di compromissione (IOC).
- Comprendere il contesto e le implicazioni delle minacce e degli attacchi alla sicurezza.
- Fornire regolarmente informazioni relative alle minacce a sicurezza, risposta agli incidenti e gestione del rischio.

Le piattaforme di intelligence sulle minacce aggregano i dati sulle minacce provenienti da diverse organizzazioni, fornendo ai team di sicurezza conoscenze esterne sulle minacce, consentendo loro di essere più proattivi, predittivi e prendere decisioni migliori. Tuttavia, poiché i dati di intelligence sulle minacce provengono spesso da centinaia di fonti, l'aggregazione manuale di queste informazioni è un'attività che richiede molto tempo.

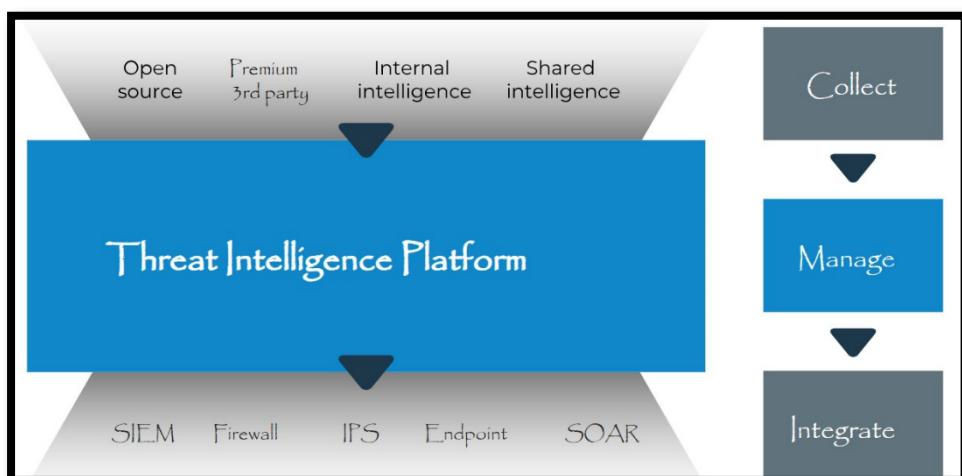


- c. Una TIP aiuta i team di sicurezza e intelligence sulle minacce:

- Automatizza, ottimizza e semplifica l'intero processo di ricerca, raccolta, aggregazione e organizzazione dei dati di intelligence sulle minacce.



- Monitora e rileva rapidamente, convalida e risponde a potenziali minacce alla sicurezza in tempo reale.
- Condivide i dati di intelligence sulle minacce con altre parti interessate tramite dashboard, avvisi, report, ecc.
- Fornisce continuamente i dati di intelligence sulle minacce più aggiornati a sistemi di sicurezza come soluzioni SIEM (Security Information and Event Management), endpoint, firewall, API (Application Programming Interface), sistemi di prevenzione delle intrusioni (IPS) e altri.



1.2 Definizione di Threat (minaccia)

Possibilità di qualsiasi terza parte di accedere a una rete di informazioni e di interferire con le relative operazioni pianificate. Le moderne minacce comuni includono:

- APT
- Phishing
- Malware
- Botnets
- Attacchi DDoS
- Ransomware

Il ricercatore di sicurezza David Bianco ha ideato un approccio intitolato

Pyramid of Pain, che delinea come causare agli avversari le maggiori

difficoltà quando attaccano la tua rete. Ciascuno dei sei livelli

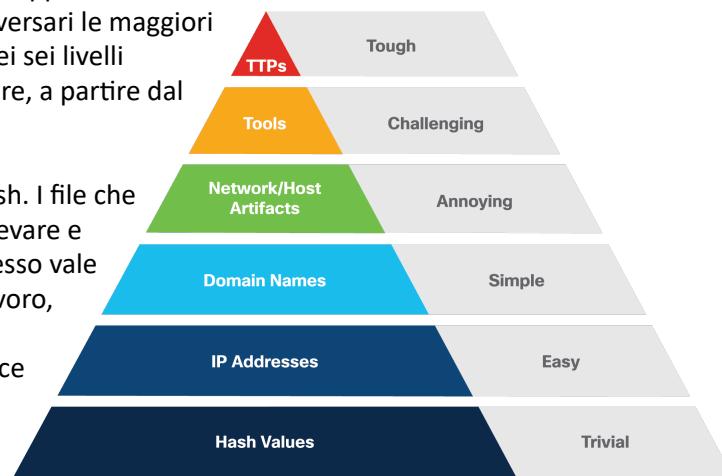
rappresenta diversi approcci che si possono adottare, a partire dal

semplice e proseguendo fino al più difficile.

Ad esempio, alla base della piramide ci sono gli hash. I file che contengono hash dannosi noti sono semplici da rilevare e anche semplici da sostituire per l'attaccante. Lo stesso vale per gli indirizzi IP, sebbene ciò richieda poco più lavoro, sia da trovare, sia da sostituire per un attaccante.

Ugualmente vale per i domini, perché è più semplice comprare un nuovo domain name.

Mentre i Network/Host artifacts sono più difficili perché il processo è human based, cioè basato sul comportamento dell'utente.



1.3 Definizione di Intelligence

Conoscenza di una minaccia acquisita dagli analisti o identificata da eventi all'interno del sistema.

Intelligence è un termine generico, ma una TIP offre agli analisti tipi di intelligence specifici e automatizzabili, tra cui:

- Conoscenza tecnica degli attacchi, compresi gli indicatori
- Finished Intelligence: il prodotto della ricerca delle informazioni disponibili da parte di esseri umani ed elaborazione di conclusioni in merito a consapevolezza situazionale, previsione delle possibili conseguenze di attacchi futuri o valutazione delle capacità degli avversari
- Human Intelligence: qualsiasi informazione raccolta dalle persone, ad esempio leggendo i forum per cercare attività sospette

Piattaforma

Un prodotto completo integrabile con strumenti e prodotti esistenti e dotato di un sistema di gestione della Threat Intelligence che automatizza e semplifica gran parte dell'attività tradizionalmente svolta dagli analisti.

2. PERCHÉ OPENCTI?

È stata utilizzata la piattaforma OpenCTI perché è facile da utilizzare e visivamente accattivante. La piattaforma ha anche connettori aggiuntivi per migliorare ulteriormente le sue capacità. Quindi è una piattaforma open-source che consente agli esperti di sicurezza informatica di condividere conoscenze utili che possono aiutare a migliorare l'intelligence sulla sicurezza informatica. In particolare, è utile per archiviare tutte le informazioni importanti che possono essere correlate a specifiche minacce informatiche. Gestisce sia i dettagli non tecnici che quelli tecnici di una minaccia, inoltre organizza le informazioni in un modo che ne renda facile la visualizzazione.



2.1 Architettura OpenCTI

Caratteristiche:

- **Grafico della conoscenza:** l'intera piattaforma si basa su un hypergraph della conoscenza che consente l'utilizzo di hyper-entities e hyper-relationships, comprese le relazioni nidificate.
- **Modello dati unificato e coerente:** dal livello operativo a quello strategico, tutte le informazioni sono collegate attraverso un modello di dati unificato e coerente basato sugli standard STIX2 (a Structured Threat Information Expression è un linguaggio e un formato di serializzazione utilizzato per scambiare informazioni sulle minacce informatiche, CTI).
- **By-design sourcing of data origin:** ogni relazione tra le entità ha attributi basati sul tempo e sullo spazio e deve essere originata da un report con un livello di confidenza specifico.
- **Gestione dell'accesso ai dati:** controllo completo della gestione dell'accesso ai dati utilizzando gruppi con autorizzazioni.

Nell'immagine sottostante possiamo vedere l'architettura di OpenCTI. Essa si basa su una serie di database per svolgere determinate funzioni, i quali a loro volta sono collegati **dall'API GraphQL** che consente ai broker di interagire con i database disponibili.

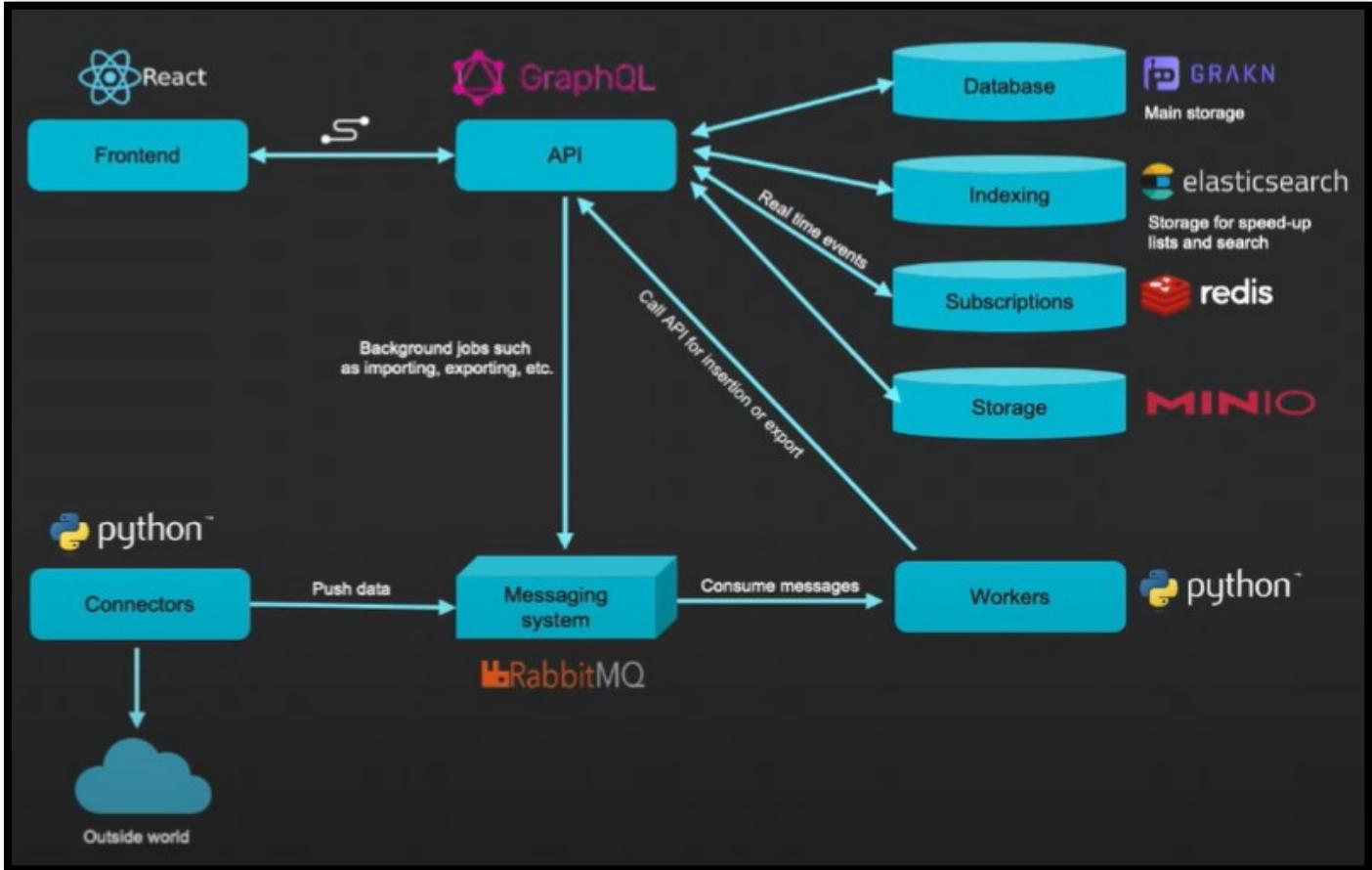
Il modo consigliato per creare o aggiornare i dati nella piattaforma OpenCTI è tramite OpenCTI **worker**. Ciò consente al connettore di inviare migliaia di entità contemporaneamente senza dover pensare all'ordine di importazione, alle prestazioni o alla gestione degli errori.

Sistema di messaggistica

Dopo che i dati sono stati convertiti in bundle STIX 2.1 JSON (un Bundle è una collezione di STIX Objects e Marking Definitions raggruppati in un singolo container), i connettori li inviano al sistema di messaggistica RabbitMQ il quale è molto scalabile. È importante capire che i fasci sono effettivamente divisi in piccoli pezzi per migliorare il parallelismo e la velocità durante l'ingestione da parte dei lavoratori.

Workers

I workers sono processi Python senza stato molto basilari che consumano messaggi STIX 2.1 (chunk) dalle code e creano gli elementi corrispondenti nella piattaforma OpenCTI utilizzando l'API GraphQL. Fondamentalmente, la capacità dei lavoratori di scrivere dati in modo efficiente è collegata alla capacità di OpenCTI di assorbirli rapidamente.



Da considerare anche il fatto che un messaggio STIX 2.1 nella coda può portare alla creazione da 1 a 10 elementi in OpenCTI (autori, etichette, riferimenti esterni, ecc.).

OpenCTI Platform

Per quanto riguarda OpenCTI, le prestazioni possono essere influenzate da 2 diversi aspetti:

- Le prestazioni del database ElasticSearch: OpenCTI si basa su ElasticSearch per archiviare i dati.
- Data Management: la piattaforma esegue molte elaborazioni sui dati ingeriti, garantendo coerenza degli identificatori, fusione di elementi come hash di file, ecc. Per questo motivo, le prestazioni dipenderanno dalle fonti di dati e dalla qualità della conoscenza stessa (relazioni, tag, ecc.).

2.2 STIX2

https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_e2e1szrqfoan

Structured Threat Information Expression (STIX™) è un linguaggio e un formato di serializzazione utilizzato per lo scambio di informazioni sulle minacce informatiche (CTI), inoltre è open source e gratuito.

Con STIX, tutti gli aspetti di sospetto, compromesso e attribuzione possono essere rappresentati con oggetti e relazioni descrittive. Le informazioni STIX possono essere rappresentate visivamente per un analista o archiviate come JSON per essere rapidamente leggibili dalla macchina.

Concatenare più oggetti insieme attraverso relazioni consente rappresentazioni facili o complesse di CTI. Di seguito è riportato un elenco di ciò che può essere rappresentato tramite STIX, in particolare gli oggetti che sono stati utilizzati nel nostro progetto:

- **Vulnerability**: un errore nel software che può essere utilizzato direttamente da un hacker per accedere a un sistema o a una rete.
- **Bundle**: è una raccolta di oggetti STIX arbitrari raggruppati in un unico contenitore.
- **ExternalReference**: i riferimenti esterni vengono utilizzati per descrivere i puntatori a informazioni rappresentate al di fuori di STIX. Ad esempio, un oggetto malware potrebbe utilizzare un riferimento esterno per indicare un ID per quel malware in un database esterno oppure un report potrebbe utilizzare riferimenti per rappresentare il materiale di origine.

- **Indicator:** contiene un modello che può essere utilizzato per rilevare attività informatiche sospette o dannose.

Altri STIX Stix Domain Objects (SDOs) sono:

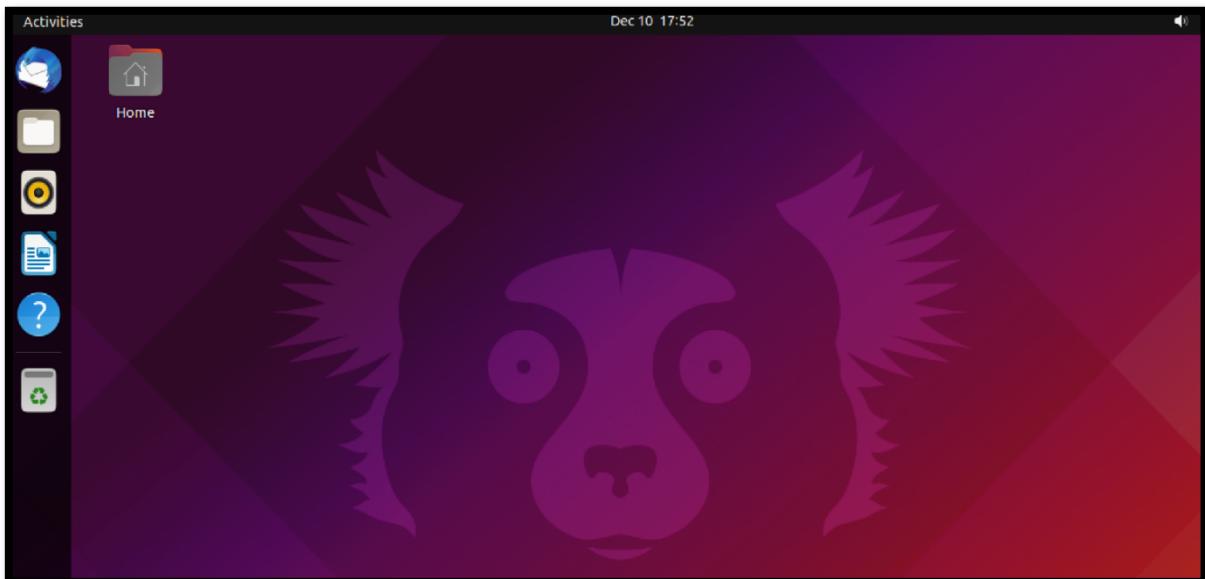
- **Identity:** individui, organizzazioni o gruppi effettivi (ad es. ACME, Inc.) nonché classi di individui, organizzazioni, sistemi o gruppi (ad es. il settore finanziario).
- **Attack Pattern:** Un tipo di TTP (Tattiche, Tecniche e Procedure) che descrive i modi in cui gli avversari tentano di compromettere gli obiettivi.
- **Campaign:** un raggruppamento di comportamenti contraddittori che descrive un insieme di attività o attacchi dannosi che si verificano in un periodo di tempo contro un insieme specifico di obiettivi.
- **Course of Action:** una raccomandazione di un produttore di intelligence a un consumatore sulle azioni che potrebbero intraprendere in risposta a tale intelligence.
- **Grouping:** afferma esplicitamente che gli oggetti STIX di riferimento hanno un contesto condiviso, a differenza di un bundle STIX (che non trasmette esplicitamente alcun contesto).
- **Infrastructure:** rappresenta un tipo di TTP e descrive qualsiasi sistema, servizio software e qualsiasi risorsa fisica o virtuale associata destinata a supportare uno scopo.
- **Intrusion Set:** un insieme raggruppato di comportamenti e risorse contraddittori con proprietà comuni che si ritiene siano orchestrati da un'unica organizzazione.
- **Location:** rappresenta una posizione geografica.
- **Malware:** un tipo di TTP che rappresenta codice dannoso.
- **Malware Analysis:** i metadati e i risultati di una particolare analisi statica o dinamica eseguita su un'istanza o famiglia di malware.
- **Note:** trasmette del testo informativo per fornire ulteriore contesto e/o per fornire analisi aggiuntive non contenute negli oggetti STIX, negli oggetti Marking Definition o negli oggetti Language Content a cui si riferisce Note.
- **Observed Data:** trasmette informazioni su entità relative alla sicurezza informatica come file, sistemi e reti utilizzando gli oggetti cyber-osservabili (SCO) di STIX.
- **Opinion:** una valutazione della correttezza delle informazioni in un oggetto STIX prodotto da un'entità diversa.
- **Report:** raccolte di informazioni sulle minacce incentrate su uno o più argomenti, come la descrizione di un attore di minacce, malware o tecnica di attacco, inclusi il contesto e i relativi dettagli.
- **Threat Actor:** individui, gruppi o organizzazioni reali che si ritiene operino con intenzioni dannose.
- **Tool:** software legittimo che può essere utilizzato dagli attori delle minacce per eseguire attacchi.

Altri Stix Relationship Objects (SROs):

- **Relationship:** utilizzato per collegare tra loro due SDO o SCO al fine di descrivere come sono correlati tra loro.
- **Sighting:** denota la convinzione che sia stato rilevato qualcosa in CTI (ad es. un indicatore, malware, strumento, attore di minacce, ecc.).

3. UBUNTU

È stata installata la versione 21.10 insieme alla GUI di Ubuntu.



Utilizzando la CMD di Windows, tramite il comando *ssh* e *indirizzo IP* ricavato dalla VM, possiamo utilizzare questa linea di comando per effettuare operazioni sulla macchina virtuale OpenCTI.

```
C:\opencti@opencti: ~
Microsoft Windows [Versione 10.0.19042.1348]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\Serafino>ssh opencti@192.168.1.8
ssh: connect to host 192.168.1.8 port 22: Connection refused

C:\Users\Serafino>ssh opencti@192.168.1.14
opencti@192.168.1.14's password:
Welcome to Ubuntu 21.10 (GNU/Linux 5.13.0-22-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

3 updates can be applied immediately.

Last login: Fri Dec 10 17:59:01 2021 from 192.168.1.14
opencti@opencti:$
```

4. OPENCTI

Il concetto principale di database di OpenCTI è quello di un **DB Graph** in cui sono presenti due diversi tipi di entità:

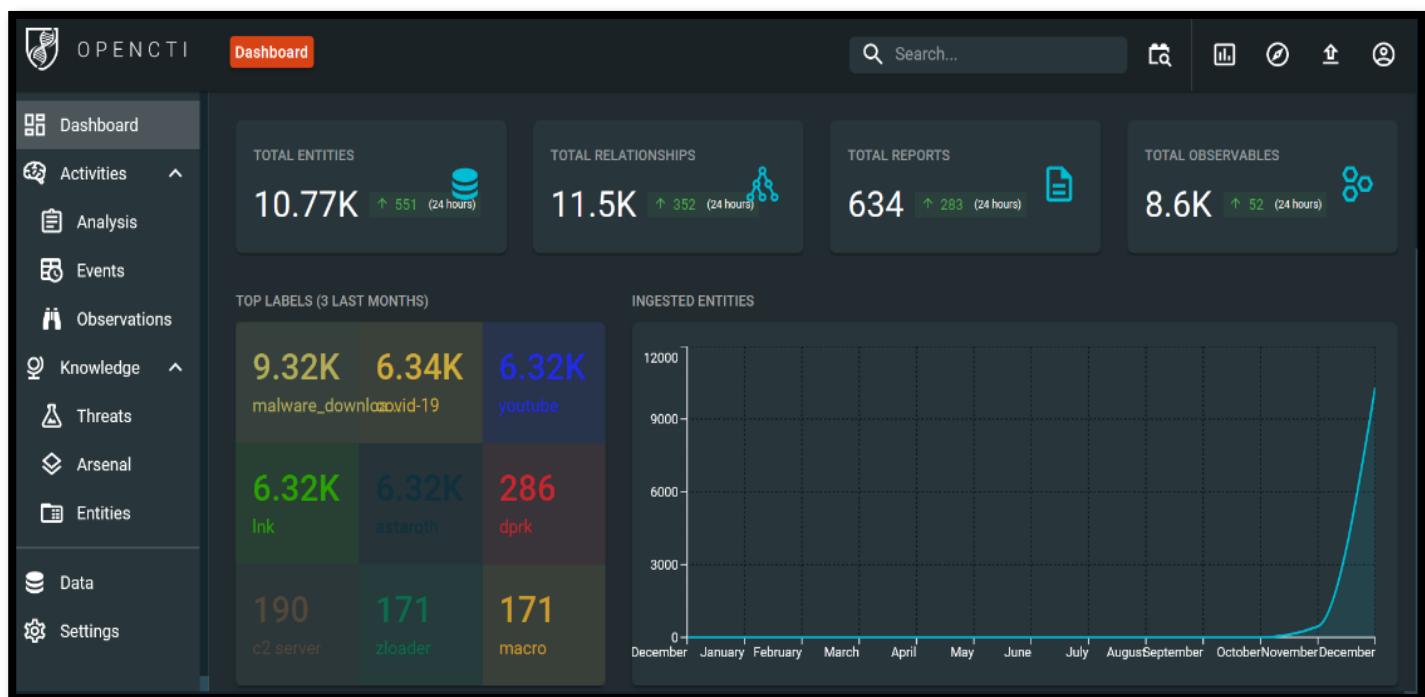
- **Nodes:** che descrivono un'entità ed i suoi valori come un indirizzo IP, un domain name o un malware.
- **Edges:** descrivono le relazioni tra due entità nodo.

Nella sezione **Dashboard** troviamo una vista generale della piattaforma in live. Come si può evincere dall'immagine, sono presenti alcuni dati forniti dai connettori, sono presenti:

- Total Entities, cioè il numero di tutte le entità presenti nella piattaforma.
- Total Relationships, indica il numero di tutte le relazioni create nella piattaforma
- Total Reports, indica il numero totale di reports nella piattaforma ed il numero di report appena raccolti.
- il totale degli osservabili, sarebbero il numero totale di osservabili nella piattaforma inclusi quelli appena raccolti.

Oltre ai valori raccolti di cui abbiamo parlato, vengono forniti all'utente anche dei grafici e mappe, come:

- Ingested entities, un grafico che indica quante entità sono state 'ingerite' e quando (mese).



Sempre all'interno della Dashboard, è presente una classifica delle TOP 10 entità attive con maggior numero di relazioni, in un periodo di osservazione pari a 3 mesi. Qui troviamo il Trojan bancario più



famoso: Emotet; uno dei motivi per cui ha avuto e continua ad avere così tanto successo è la sua costante evoluzione nelle tecniche di attacco. Un esempio è il fatto che utilizza gli allegati di posta elettronica rubati per aggiungere credibilità allo spam che genera per infettare sistemi mirati.

Sulla destra, invece, troviamo una mappa con i Targeted countries, definita di default in OpenCTI, ed utilizzata per mostrare l'intensità del targeting; cioè il numero di relazioni verso i paesi. Si possono distinguere 3 colori: arancione, per un targeting 'pesante', arancione pallido per un targeting medio ed infine giallo per un targeting basso.

Come indicato dalla guida di OpenCTI, è stato creato un utente per ogni singolo connettore.

Name	Email	Firstname	Lastname	Creation Date
abuse	sd@g.vb			Nov 30, 2021 >
admin	admin@openciti.io	Admin	OpenCTI	Oct 24, 2021 >
alienVault	32@email.com			Nov 30, 2021 >
amitt	11@email.com			Nov 30, 2021 >
cryptolaemus	12@email.com			Nov 30, 2021 >
cuckoo	45@email.it			Nov 30, 2021 >
cve	21@email.com			Nov 30, 2021 >
Cyber Threat Coalition	444@email.com			Nov 30, 2021 >

5. INSTALLAZIONE CONNETTORI

La tabella seguente offre una panoramica degli attuali tipi di connettori e di alcuni casi d'uso tipici:

Name	Typical Use Cases	OpenCTI flag	Example Connector
External Import	Integrate external TI provider Integrate external TI platform	EXTERNAL_IMPORT	Alienvault
Internal Import File	(Bulk) import knowledge from files	INTERNAL_IMPORT_FILE	Import Report
Internal Export File	(Bulk) export knowledge to files	INTERNAL_EXPORT_FILE	Export File CSV
Internal Enrichment	Enhance existing data with additional knowledge	INTERNAL_ENRICHMENT	AbuseIP
Stream	Integrate external TI platform Integrate external TI provider	STREAM	Elastic

Lista dei connettori che abbiamo installato sulla piattaforma:

Un connettore in OpenCTI è un servizio che viene eseguito accanto alla piattaforma e può essere implementato in quasi tutti i linguaggi di programmazione che supportano il formato STIX2. I connettori vengono utilizzati per estendere le funzionalità di OpenCTI e consentire agli operatori di spostare parte del carico di lavoro di elaborazione su servizi esterni.

Per quanto riguarda le prestazioni dei connettori, esse dipenderanno dalle API/feed dei sistemi remoti e dall'implementazione del connettore. Alcuni connettori scaricano regolarmente API di servizi esterni e quindi convertono i dati ricevuti in bundle STIX 2.1 JSON, altri consumeranno feed in tempo reale con dati già formattati utilizzando lo standard STIX.

The screenshot shows the OpenCTI web application. The top navigation bar includes links for Entities, Background tasks, Connectors (highlighted in red), Synchronization, Data sharing, and a search bar. The left sidebar contains a tree view of the system's components: Dashboard, Activities (Analysis, Events, Observations), Knowledge (Threats, Arsenal), Entities, Data, and Settings. The main content area is titled 'Registered connectors' and lists ten entries:

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	MODIFIED
1	AM!TT Dec 10, 2021, 7:35:13 PM	Data import	NOT APPLICAB...	25.66K	
2	Abuse.ch URLhaus Dec 10, 2021, 7:35:49 PM	Data import	NOT APPLICAB...	95.91K	
3	AbuseIPDB Dec 10, 2021, 7:35:50 PM	Enrichment	AUTOMATIC	0	
4	AlienVault Dec 10, 2021, 7:35:49 PM	Data import	NOT APPLICAB...	2.15K	
5	BackupFiles Dec 10, 2021, 7:35:46 PM	Streaming	NOT APPLICAB...	0	
6	Common Vulnerabilities and Exposures Dec 10, 2021, 7:35:16 PM	Data import	NOT APPLICAB...	0	
7	Cryptolaemus Dec 10, 2021, 7:35:19 PM	Data import	NOT APPLICAB...	0	
8	CyberThreatCoalition Dec 10, 2021, 7:35:42 PM	Data import	NOT APPLICAB...	0	

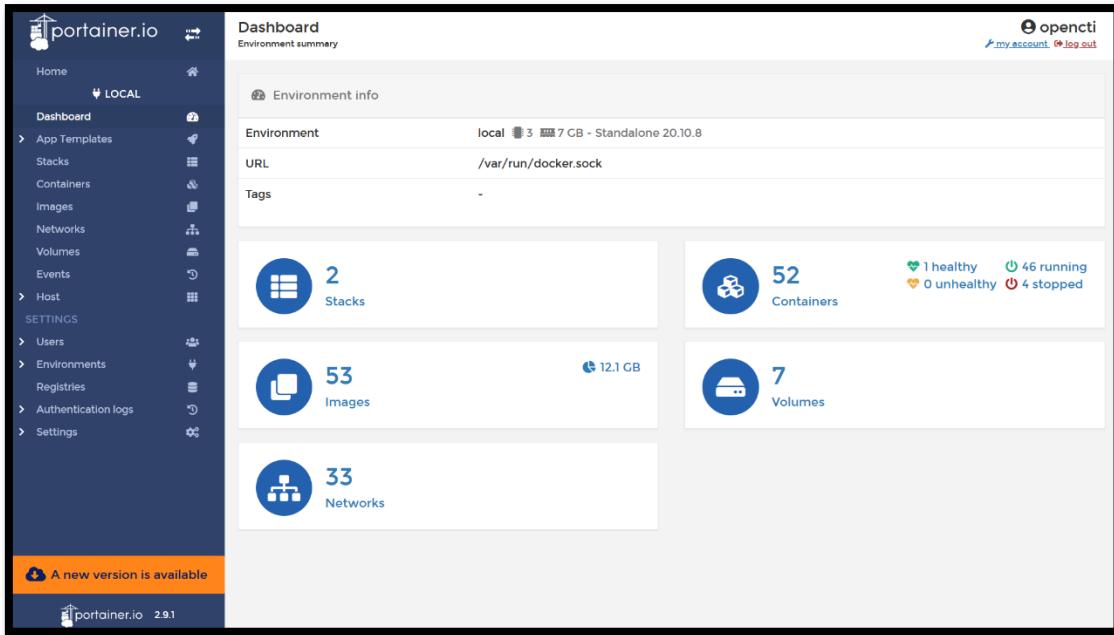
Questo è ALIENVAULT, uno dei connettori installati, mentre elabora le operazioni.

The screenshot shows the detailed view of the ALIENVAULT connector. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled 'ALIENVAULT' and has a status indicator 'ACTIVE'. It is divided into several sections:

- BASIC INFORMATION:** Includes fields for Type (EXTERNAL_IMPORT), Last update (Dec 10, 2021, 7:40:44 PM), Only contextual (NOT APPLICAB...), Automatic trigger (NOT APPLICAB...), and Scope (alienvault).
- DETAILS:** Shows State ({"latest_pulse_timestamp": "2021-12-10T00:03:02.865000", "last_run": 1639161152}), Listen queue (listen_0d77e071-413d-4f27-b5f6-8850ae834e34), Push queue (push_0d77e071-413d-4f27-b5f6-8850ae834e34), and a 'DELETE' button.
- IN PROGRESS WORKS:** Lists two runs:
 - AlienVault run @ 2021-12-10 18:01:26: Status IN PROGRESS, Operations completed 894, Total number of operations 2932, Progress bar (mostly green).
 - AlienVault run @ 2021-12-03 17:36:28: Status IN PROGRESS, Operations completed 0, Total number of operations 588969, Progress bar (mostly green).

6. PORTAINER

Per installare i vari connettori abbiamo utilizzato Docker-Compose e nel gestirli abbiamo utilizzato il portale Portainer.io, che fornisce uno Stack che ci permette di collegare e gestire in un unico file tutti i connettori.



Riprendendo sempre il connettore ALIENVULT, qui è mostrato il suo file docker-compose, dove sono stati inseriti l'URL di OpenCTI, il token dell'utente creato, un UUID4 e l'API key richiesta (ottenuta grazie all'iscrizione al sito ALIENVULT).

Naturalmente questa operazione è stata ripetuta per tutti i connettori, stando attenti a non creare nessun conflitto.

The screenshot shows the Portainer.io Stack editor with the following docker-compose.yml content:

```
version: '3.8'
services:
  connector-alienvault:
    image: opencti/connector-alienvault:rolling
    environment:
      - OPENCTI_URL=http://opencti:8080
      - OPENCTI_TOKEN=3d64630f-d5dd-47c1-ba4e-b15295f2655b
      - CONNECTOR_ID=0d77e071-413d-4f27-b5f6-8850ae834e34
      - CONNECTOR_TYPE=EXTERNAL_IMPORT
      - CONNECTOR_NAME=AlienVault
      - CONNECTOR_SCOPE=alienvault
      - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
      - CONNECTOR_UPDATE_EXISTING_DATA=false
      - CONNECTOR_LOG_LEVEL=info
      - ALIENVULT_BASE_URL=https://ctx.alienvault.com
      - ALIENVULT_API_KEY=477e2c2545c1a98dc82af9c430cf4be79142fd9131526b54fba8b01506251eb
      - ALIENVULT_TLP=White
      - ALIENVULT_CREATE_OBSERVABLES=true
      - ALIENVULT_CREATE_INDICATORS=true
      - ALIENVULT_PULSE_START_TIMESTAMP=2020-05-01T00:00:00
      - ALIENVULT_REPORT_TYPE=threat-report
      - ALIENVULT_REPORT_STATUS>New
      - ALIENVULT_GUESS_MALWARE=false
      - ALIENVULT_GUESS_CVE=false
      - ALIENVULT_EXCLUDED_PULSE_INDICATOR_TYPES=FileHash-MD5,FileHash-SHA1
      - ALIENVULT_ENABLE_RELATIONSHIPS=true
    # BEWARE! Could be a lot of data
    # Use tags to guess malware
    # Use tags to guess CVE
    # Excluded Pulse indicator types
    # Enable/Disable relationships
```

Questa è la lista dei Container che permettono l'installazione dei connettori alla piattaforma OpenCTI.

	Name	State	Quick actions	Stack	Image
	opencti_minio_1	healthy	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	minio/minio:RELEASE.2021-10-13T00-23-17Z
	opencti_connector-intezer-sandbox_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-intezer-sandbox:rolling
	opencti_connector-opencti_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-opencti:rolling
	opencti_connector-mandiant_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-mandiant:rolling
	opencti_connector-misp_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-misp:rolling
	opencti_connector-ivre_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-ivre:rolling
	opencti_connector-vxvault_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-vxvault:rolling
	opencti_connector-malpedia_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-malpedia:rolling
	opencti_connector-elastic_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-elastic:rolling
	opencti_connector-ipinfo_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-ipinfo:rolling
	opencti_connector-cuckoo_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-cuckoo:rolling
	opencti_connector-cybercrime..._1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-cybercrime-tracker:rolling
	opencti_connector-hygiene_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-hygiene:rolling
	opencti_connector-tanium_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-tanium:rolling
	opencti_connector-greynoise_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-greynoise:rolling
	opencti_connector-shodan_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-shodan:rolling
	opencti_connector-valhalla_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-valhalla:rolling
	opencti_connector-virustotal_1	running	☰ ⚡ ⚡ ⚡ ⚡ ⚡	opencti	opencti/connector-virustotal:rolling

7. CONNETTORI CUSTOM

7.1 CVE Trends



CVE Trends

Creata dall' ingegnere e ricercatore di cybersecurity **Simon J.Bell** (<https://twitter.com/simonbyte>), **CVE Trends** pone la sua attenzione sul monitorare i trend di vulnerabilità presenti su Twitter.

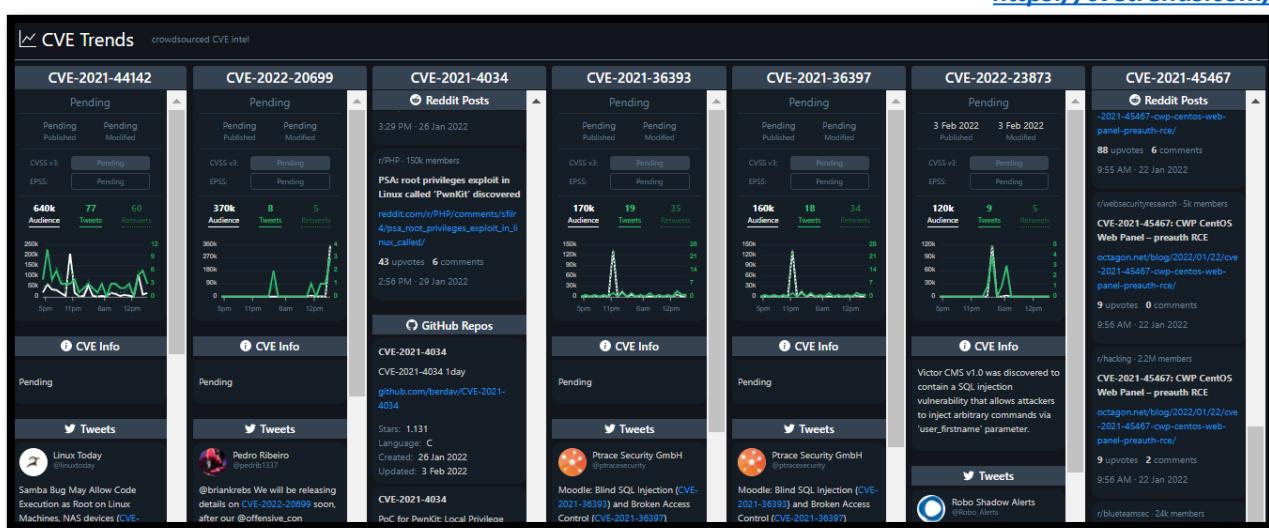
Esso raccoglie informazioni in tempo reale sui CVE twittati con intervalli settimanali e/o orari.

Il meccanismo si basa sul crowdsourcing di CVE dalla *filtered stream API di Twitter* combinandolo con i dati delle API di **Reddit**, **Github**, **NIST NVD** (contenente le info specifiche di ogni CVE analizzato).

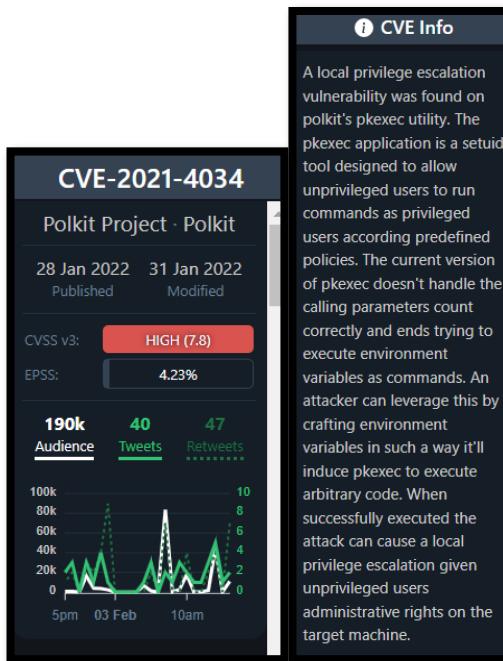
Il back-end è costruito in Phyton, Flask, PostgreSQL e Redis, in esecuzione su NGINX e Ubuntu.

Il front-end è costruito in HTML5, CS3, React e Bootstrap.

<https://cvetrends.com/>



7.1.1 Come si compone un CVE Trend



Un CVE Trend, riprendendo il concetto di CVE racchiude le informazioni su una falla nella sicurezza informatica divulgata al pubblico. Essa si compone principalmente di uno **Score** e di una **Severity** che ne forniscono il livello di pericolosità. La sezione *Info* fornisce una breve descrizione della *Common Vulnerabilities and Exposures* (CVE).

The figure shows three panels of social media posts related to CVE-2021-4034:

- Tweets:** A post by user @ZZKLLX (@ZZKLLX) stating they are checking if their Linux system is vulnerable to the CVE-2021-4034 exploit. They mention patches have been applied. The post includes a link to a news article and has 9 Retweets and 19 Likes.
- Reddit Posts:** A post in the r/archlinux subreddit discussing a major exploit for CVE-2021-4034 that allows privilege escalation. It links to a bleepingcomputer.com news article and has 107 upvotes and 11 comments.
- GitHub Repos:** A list of GitHub repositories related to CVE-2021-4034, including one for PwnKit and another for the exploit itself.

Ogni sezione relativa ad un CVE presenta dei campi di ricerca dei Tweet, dei Repos su GitHub o dei post su Reddit

7.1.2 Composizione del 'docker-compose' file

COMPONENTE	ATTRIBUTO	FUNZIONALITA'
OPENCTI_URL	http://opencti:8080	Url di accesso alla piattaforma OpenCTI
OPENCTI_TOKEN	ChangeMe	Token personalizzato e necessario per far partire il connettore
CONNECTOR_ID	ChangeMe	Stringa personalizzata UUID 4 usata come identificativo
CONNECTOR_TYPE	EXTERNAL_IMPORT	Tipo di connettore analizzato
CONNECTOR_NAME	Cve Trends	Nome del connettore
CONNECTOR_SCOPE	Vulnerability	Riferimento a oggetto Stix importato nella piattaforma
CONNECTOR_CONFIDENCE_LEVEL	100	Livello di trust(0-100)
CONNECTOR_LOG_LEVEL	Info	Livello dei Log

7.1.3 Analisi dei punti salienti del codice

```

def convert(self, filename):
    # Create the default author
    author = Identity(name="Cve Trends")
    PRE_LINK = "https://nvd.nist.gov/vuln/detail/"
    # count = 0
    # with open(filename) as json_file:
    #     vulnerabilities_bundle = [author]
    #     html = requests.get(filename).text
    #     data = json.loads(html)
    #     dati = data.get('data')
    #     for cves in dati:
    #
    #         exter = PRE_LINK+cves.get('cve')
    #         name = cves.get('cve')
    #         cvssv3_base_score = cves.get('cvssv3_base_score')
    #         cvssv3_base_severity = cves.get('cvssv3_base_severity')
    #         description = cves.get('description')

```

In questa fase , nel metodo **Convert** si definisce l'autore e la prima parte di stringa (**PRE_LINK**)che sarà utilizzata per raggiungere l'elemento di report inserito tra gli External Reference (**exter**) .

Si ricava inoltre il *json* della pagina html sfruttando il passaggio dell'url della singola CVE in twitter (**url**) nella variabile **filename** :

<https://twitter.com/ +twitter user handle+/status/+tweet id>
Ricavato il json si ricercano le singole informazioni per ogni CVE al suo interno

```

#Creo External references
    external_reference = ExternalReference(
        source_name="NIST NVD", url=exter
    )
    external_references=[external_reference]
#prendo gli url di git
github=cves.get('github_repos')
for gitin in github:
    url=gitin.get('url')
    external_reference1 = ExternalReference(
        source_name="Git hub",url=url
    )
    external_references.append(external_reference1)
tweets=cves.get('tweets')
for tweet in tweets:
    tweet_id=tweet.get('tweet_id')
    twitter_user_handle=tweet.get('twitter_user_handle')
    url="https://twitter.com/"+twitter_user_handle+"/status/"+tweet_id
    external_reference2= ExternalReference(
        source_name="Tweet",url=url
    )
    external_references.append(external_reference2)
reddit_posts=cves.get('reddit_posts')
for reddit_post in reddit_posts:
    reddit_url=reddit_post.get('reddit_url')
    external_reference3 = ExternalReference(
        source_name="Reddit", url=reddit_url
    )
    external_references.append(external_reference3)

```

Vengono in questa successiva fase importate le informazioni rispettivamente per *NIST NVD*, *Github*, *Twitter* e *Reddit* presenti all'interno del file json ricavato precedentemente per ogni CVE. Queste in seguito vengono aggiunte nelle *external_references* che verranno dal connettore presentate sulla piattaforma.

```

# Creating the vulnerability with the extracted fields
vulnerability = Vulnerability(
    id=OpenCTIStix2Utils.generate_random_stix_id("vulnerability"),
    name=name,
    description=description,
    created_by_ref=author,
    external_references=external_references,
    custom_properties={
        "x_openccti_base_score": cvssv3_base_score,
        "x_openccti_base_severity": cvssv3_base_severity,
    },
)
# Adding the vulnerability to the list of vulnerabilities
vulnerabilities_bundle.append(vulnerability)

```

Qui invece si creano, sfruttando il formato STIX2 **Vulnerability**, le vulnerabilità inserendo:

- l'identificativo
- il nome
- la descrizione
- l'*external_reference*
- come *Custom Properties* lo **Score** e la **Severity** ricavate da ogni CVE all'interno di CVE Trends

```
# Creating the bundle from the list of vulnerabilities
bundle = Bundle(objects=vulnerabilities_bundle, allow_custom=True).serialize()
return bundle
```

Si serializza qui il **Bundle Stix2** contenente tutte le **vulnerabilità** create

```
def convert_and_send(self, url, work_id):
    try:

        # Converting the file to stix2
        self.helper.log_info("Converting the file")

        bundle = self.convert(url)

        self.helper.send_stix2_bundle(
            bundle,
            work_id=work_id,
        )
```

Utilizzando **send_stix2_bundle** si invia il **Bundle** alla piattaforma OpenCTI

7.2 UrlscanIo



Fondato dallo sviluppatore Johannes Gilger (<https://urlscan.io/about/>)

URLscan. io è un servizio gratuito per scansionare e analizzare siti web.

Quando un URL viene inviato a urlscan.io, un processo automatizzato navigherà verso l'URL come un normale utente e registrerà l'attività creata dalla navigazione di questa pagina. Ciò include i domini e gli IP contattati, le risorse (JavaScript, CSS, ecc.) richieste da tali domini, nonché ulteriori informazioni sulla pagina stessa.

urlscan.io acquisirà uno screenshot della pagina, registrerà il contenuto del DOM, le variabili globali JavaScript, i cookie creati dalla pagina e altre osservazioni. Se il sito prende di mira gli utenti uno degli oltre 400 marchi monitorati da urlscan.io, verrà evidenziato come potenzialmente dannoso nei risultati della scansione.

<https://urlscan.io/>

A screenshot of the urlscan.io homepage. At the top, there's a dark navigation bar with the urlscan.io logo, a search icon, and links for Home, Search, Live, API, Blog, Docs, Pricing, and a user profile for Jacopo. To the right, it says "Sponsored by SecurityTrails". Below the bar, the main heading "urlscan.io" is displayed in large green letters, with the subtitle "A sandbox for the web" underneath. A search bar labeled "URL to scan" is centered. To its right are two buttons: a teal "▶ Public Scan" button and a grey "Options" button. Below this, a section titled "Recent scans" shows three entries: "www.forbes.com/profile/larry-page/" (16 seconds ago, 4 MB, 41 IPs, 7 domains, 2 flagged), "notes.io/Uqmu" (16 seconds ago, 491 KB, 55 IPs, 11 domains, 3 flagged), and "51.38.196.71/" (20 seconds ago, 128 KB, 12 IPs, 3 domains, 2 flagged). Each entry includes a small lock icon and a preview thumbnail.

7.2.1 Di cosa si compone una ricerca UrlscanIo

www.unisannio.it 35.152.60.177 

Submitted URL: <http://www.unisannio.it/>
 Effective URL: <https://www.unisannio.it/>
 Submission: On February 03 via manual (February 3rd 2022, 6:35:03 pm UTC) from IT  – Scanned from IT 

[Summary](#) [HTTP 120](#) [Redirects](#) [Links 22](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#)

[Live screenshot](#) [Full image](#)

Summary

This website contacted 6 IPs in 3 countries across 5 domains to perform 120 HTTP transactions. The main IP is **35.152.60.177**, located in Milan, Italy and belongs to **AMAZON-02, US**. The main domain is www.unisannio.it.

TLS certificate: Issued by TERENA SSL CA 3 on January 16th 2020. Valid for: 2 years.

www.unisannio.it scanned 9 times on urlscan.io [Show Scans 9](#)

urlscan.io Verdict: No classification 

Live information

Google Safe Browsing:  No classification for www.unisannio.it
 Current DNS A record: 35.152.60.177 (AS16509 - AMAZON-02, US)



Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
113	IP Address 35.152.60.177  16509 (AMAZON-02)					
1	2a00:1450:4001:813::2008  15169 (GOOGLE)					
4	2a06:98c1:3120::7  13335 (CLOUDFLARENET)					
2	2a00:1450:4001:80f::200e  15169 (GOOGLE)					
1	2606:4700::6811:f349  13335 (CLOUDFLARENET)					
120		6				

Page URL History [Show full URLs](#)

1. <http://www.unisannio.it/>  <https://www.unisannio.it/> [Page URL](#)

Detected technologies

-  [Drupal](#) (CMS) [Expand](#)
-  [Bootstrap](#) (Web Frameworks) [Expand](#)
-  [Font Awesome](#) (Font Scripts) [Expand](#)
-  [Google Analytics](#) (Analytics) [Expand](#)
-  [Google Tag Manager](#) (Tag Managers) [Expand](#)
-  [jQuery](#) (JavaScript Libraries) [Expand](#)

Page Statistics

120	100 %	80 %	5	5
Requests	HTTPS	IPv6	Domains	Subdomains
6	3	3608 kB	5007 kB	4
IPs	Countries	Transfer	Size	Cookies

UrlScan.io presenta in questo specifico caso di www.unisannio.it nell'ordine :

- L'url e il Dominio
- L'indirizzo IP
- Un summary di riferimento a passate ricerche effettuate per lo stesso sito
- Una classificazione della eventuale pericolosità (qui "No Classification")
- Un live Screenshot della pagina
- Domini di appartenenza
- Statistiche varie sulla pagina

7.2.2 Analisi del 'docker-compose' file

COMPONENTE	ATTRIBUTO	FUNZIONALITA'
OPENCTI_URL	http://opencti:8080	Url di accesso alla piattaforma OpenCTI
OPENCTI_TOKEN	ChangeMe	Token personalizzato e necessario per far partire il connettore
CONNECTOR_ID	ChangeMe	Stringa personalizzata UUID 4 usata come identificativo
CONNECTOR_TYPE	INTERNAL_ENRICHMENT	Tipo di connettore analizzato
CONNECTOR_NAME	UrlScanIo	Nome del connettore
CONNECTOR_SCOPE	Url,Ipv4-Addr,Ipv6-Addr,X-OpenCTI-Hostname,Domain-Name	Riferimento a oggetto Stix importato nella piattaforma
CONNECTOR_CONFIDENCE_LEVEL	100	Livello di trust (0-100)
CONNECTOR_LOG_LEVEL	info	Livello dei Log
URLSCANIO_API_KEY	ChangeMe	API Key personale necessaria per l'uso del connettore
URLSCANIO_MAX_TLP	TLP:AMBER	Colore specifico per label
CONNECTOR_AUTO	true	Boolean per il trigger automatico del connettore

7.2.3 Analisi dei punti salienti del codice di UrlscanIo

```

def _process_observable(self, observable):
    self.helper.log_info(
        "Processing the observable " + observable["observable_value"]
    )

    if observable["entity_type"] in ["Url", "IPv4-Addr", "IPv6-Addr", "X-OpenCTI-Hostname", "Domain-Name"]:
        return self._submit_url(observable)
    
```

Il connettore di **Enrichment**, come poi sarà visibile nei casi d'uso, viene utilizzato esclusivamente per le entità definite dell'array di **observables**.

```

def _submit_url(self, observable):
    self.helper.log_info("Observable is a URL, triggering the sandbox...")
    values = observable["value"]

    headers = {'API-Key': self.api_key, 'Content-Type': 'application/json'}
    data = {"url": values, "visibility": "public"}
    response = requests.post('https://urlscan.io/api/v1/scan/', headers=headers, data=json.dumps(data))
    res = response.json()
    api = res.get('api')
    time.sleep(15)
    html = requests.get(api).text
    data = json.loads(html)

    self._send_knowledge(observable, data)

```

La fase iniziale si basa sullo sfruttare l'Api-key definita nel file di configurazione del connettore per poter poi ricavare il file json dall' Api di urlscan.io di cui verranno ricavate le informazioni necessarie per lo specifico url del singolo *observable* (in url:"**values**") .

E' importante sottolineare come sia necessario un **time.sleep** di 15 secondi affinchè si dia il tempo necessario di caricamento di tutti i campi nel json e si eviti al connettore una prematura ricerca all'interno dello stesso.

```

def _send_knowledge(self, observable, report):

    final_observable = observable
    ob_id=final_observable["standard_id"]
    verdict = report.get('verdicts')
    if verdict is not None:
        overall = verdict.get('overall')
        malicious = overall.get('malicious')
        if malicious == True :
            tag_ha = self.helper.api.label.create(value="Malicious", color="#f44336")
            self.helper.api.stix_cyber_observable.add_label(
                id=ob_id, label_id=tag_ha["id"])
        )
        lists = report.get('lists')
        if lists is not None:
            countries = lists.get('countries')
            for c in countries:
                tag_c = self.helper.api.label.create(value=c, color="#ffff00")
                self.helper.api.stix_cyber_observable.add_label(
                    id=ob_id, label_id=tag_c["id"])
            )
        score = overall.get('score')
        urlscan_verdict = verdict.get('urlscan')
        categories = urlscan_verdict.get('categories')
        #Aggiungo i labels alla pagina
        for tag in categories:
            tag_ha = self.helper.api.label.create(value=tag, color="#0059f7")
            self.helper.api.stix_cyber_observable.add_label(
                id=ob_id, label_id=tag_ha["id"])
        )
    else :
        score=0
    task = report.get('task')
    reportURL = task[reportURL]
    if reportURL is None:
        return "Url, IP, hostname analizzato non valido"
    screen = task["screenshotURL"]
    self.helper.log_info("Errore dovuto a un campo preso da json")

```

La fase

permette di individuare una serie di informazioni nel json per il singolo observable:

- Il **verdetto** da cui ricavare l'**overall** e il campo **malicious**
- una label per indicare se esso è considerato **Malicious**
- una lista delle **nazioni** legate ai domini di appartenenza con rispettive label
- Lo **score** (es. 100% per Malicious)
- Le **categorie** come “phishing”, “malware”, etc. con rispettiva label
- Un live **Screenshot** della pagina web dell'*observable* (da usare per l'*external reference*)

seguente

```

#Metto nella descrizione le statistiche
stats = report.get('stats')
secureRequest = stats.get('secureRequests')
securePercentage = stats.get('securePercentage')
IPv6Percentage = stats.get('IPv6Percentage')
uniqCountries = stats.get('uniqCountries')
totalLinks = stats.get('totalLinks')
adBlocked = stats.get('adBlocked')
stringa ="secure request:"+str(secureRequest)+", secure percentage:" + str(securePercentage) +", IPv6 percentage:" +
#Aggiorno lo score
self.helper.api.stix_cyber_observable.update_field(
    id=ob_id,
    input={"key": "x_opencti_score", "value": str(score)},

)
#Aggiungo statistiche nella descrizione
self.helper.api.stix_cyber_observable.update_field(
    id=ob_id,
    input={"key": "x_opencti_description", "value": stringa},

```

Nella parte di **description** del connettore sono inserite invece le statistiche ricavate dal json con rispettivi risultati e percentuali inserite in una stringa cumulativa
Sono quindi in seguito inseriti nei campi di *score* e *description* le rispettive informazioni.

```

# Create external reference report
external_reference = self.helper.api.external_reference.create(
    source_name="Urlscan.io",
    url= reportURL ,
    description="Report di Urlscan.io",
)
self.helper.api.stix_cyber_observable.add_external_reference(
    id=ob_id,
    external_reference_id=external_reference[ "id"],
)
#Create external reference screen shot
external_reference = self.helper.api.external_reference.create(
    source_name="Screen Shot",
    url= screen ,
    description="Screen Shot di Urlscan.io",
)
self.helper.api.stix_cyber_observable.add_external_reference(
    id=ob_id,
    external_reference_id=external_reference[ "id"],
)

```

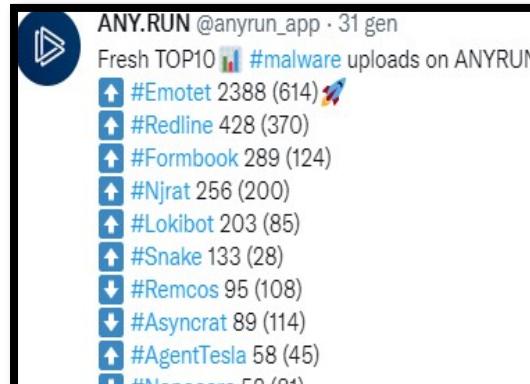
Si creano a questo punto per completezza gli `external_reference` per:

- **Report URL** della pagina
- **ScreenShot** di riferimento

7.3 IOCTweet

IOCTweet si propone di catturare gli IOC presenti su Twitter a partire da una lista di top 10 Malware pubblicata da

@anyrun_app. AnyRun fornisce un servizio di Malware Trends Tracker, che contiene articoli dinamici su vari tipi di malware. ANY_RUN sandbox elabora milioni di campioni dalla community e tali informazioni vengono visualizzate negli articoli in tempo reale, tiene traccia del malware che sta guadagnando popolarità e permette di ricevere gli ultimi IP, hash o domini. I vari IOC sono catalogati in uno dei 4 tipi, come mostrato nella figura sottostante.



Categories of Indicators of Compromise

- Understanding IoCs helps security professionals to quickly detect the threats against the organization and protect the organization from evolving threats

For this purpose, IoCs are divided into four categories:

Email Indicators	Network Indicators	Host-Based Indicators	Behavioral Indicators
<ul style="list-style-type: none">Email indicators are used to send malicious data to the target organization or individualExamples include the sender's email address, email subject, and attachments or links	<ul style="list-style-type: none">Network indicators are useful for command and control, malware delivery, identifying the operating system, and other tasksExamples include URLs, domain names, and IP addresses	<ul style="list-style-type: none">Host-based indicators are found by performing an analysis of the infected system within the organizational networkExamples include filenames, file hashes, registry keys, DLLs, and mutex	<ul style="list-style-type: none">Behavioral indicators of compromise are used to identify specific behavior related to malicious activitiesExamples of behavioral indicators include document executing PowerShell script, and remote command execution

IOCTweet raccoglie tutti i Tweet che contengono IOC e i quali appartengono ad uno dei Top10 Malware pubblicati da AnyRun, successivamente le informazioni raccolte vengono categorizzate come:

- hash files (SHA-1, MD5, SHA-256)
- Hostnames
- Domain name
- Urls
- IPv4 Address

7.3.1 Composizione del 'docker-compose' file

COMPONENTE	ATTRIBUTO	FUNZIONALITA'
OPENCTI_URL	http://opencti:8080	Url di accesso alla piattaforma OpenCTI
OPENCTI_TOKEN	ChangeMe	Token personalizzato e necessario per far partire il connettore
CONNECTOR_ID	ChangeMe	Stringa personalizzata UUID 4 usata come identificativo
CONNECTOR_TYPE	EXTERNAL_IMPORT	Tipo di connettore analizzato
CONNECTOR_NAME	Cve Trends	Nome del connettore
CONNECTOR_SCOPE	Vulnerability	Riferimento a oggetto Stix importato nella piattaforma
CONNECTOR_CONFIDENCE_LEVEL	100	Livello di trust (0-100)
CONNECTOR_LOG_LEVEL	Info	Livello dei Log
IOCTweet_INTERVAL	2	Valore maggiore di 1 che indica dopo quanti giorni effettuare un update dei dati
IOCTweet_Consumer_Key	ChangeMe	Prima credenziale per accedere all'API di Twitter
IOCTweet_Consumer_Secret	ChangeMe	Seconda credenziale per accedere all'API di Twitter
IOCTweet_Acess_Token	ChangeMe	Primo token di accesso che specifica l'account Twitter per cui viene effettuata la richiesta (per ottenerlo è necessario prima concedere l'accesso)
IOCTweet_Acess_Token_Secret	ChangeMe	Secondo token di accesso che specifica l'account Twitter per cui viene effettuata la richiesta (per ottenerlo è necessario prima concedere l'accesso)

2. Analisi dei punti salienti del codice

Per filtrare correttamente le informazioni importate da Twitter sono state implementate alcune funzioni:

La ricerca degli IOC necessita del metodo di verifica degli Url (**find_IOC**), definito dopo e di una funzione che, se la stringa considerata ha una lunghezza superiore a trenta caratteri, permetterà di individuare un hash che sarà in seguito analizzato.

Il metodo **verify_ip_url** permette di distinguere gli url e gli indirizzi IP per evitare errati inserimenti negli array appositi. Inoltre, a seguito dell'individuazione dei campi "www." e "http", viene fatta una 'pulizia' della stringa (url) tramite il metodo "clean_ip_url" (campi come "[" o "]" di fatti evitano il "click" diretto sull'url). La stringa pulita verrà aggiunta all' array specifico.

```
#Function to verify if a string is a ip address or a url
def verify_ip_url(self,stringa):
    for s in stringa:
        value = 0
        if s.isnumeric() or s == "." or s == "]" or s == "[":
            value = 0
        else:
            value=1
            break
    if value == 1:
        stringa = self.clean_ip_url(stringa)
        if stringa[0:4] == "www.":
            hostnames.append(stringa)
        elif stringa[0:4] == "http":
            urls.append(stringa)
        else:
            domain_names.append(stringa)
    elif value==0 and stringa not in ipv4_addrs:
        stringa = self.clean_ip_url(stringa)
        ipv4_addrs.append(stringa)

#find the IOC type
def find_IOC(self,string):
    array_strings = string.split(None)
    for s in array_strings:
        h = 0
        if ".]" in s or "[." in s or s[0:4]=="http":
            #print("Stampa url presa:" +s)
            self.verify_ip_url(s)
        elif len(s)>30:
            self.verify_hash(s)
```

```
#verify if a string is an hash
def verify_hash(self, stringa):
    for s in stringa:
        value = 0
        if s.isnumeric() or s.isalpha():
            value=1
        else:
            value=0
            break
    if value == 1 and stringa not in hashes and not re.search(u'\u4e00-\u9fff', stringa):
        val = find_hash(stringa)
        if val == 1:
            hashes.append(stringa)
```

Nell'immagine mostrata sopra viene applicato un filtraggio carattere per carattere; nel caso in cui tutti i caratteri della stringa (hash) passata come parametro sono tutti numeri o caratteri alfabetici allora si applica una seconda verifica, questo perché spesso alcuni caratteri (per esempio caratteri CJK) superano i vincoli del primo filtro. Infine, l'hash trovato verrà aggiunto al corrispettivo array.

```

def send_bundle(self,melf_key):
    global bundleobj
    if len(urls) !=0 :
        for patter in urls:
            url_stix = SimpleObservable(
                id=OpenCTIStix2Utils.generate_random_stix_id(
                    "x-opencti-simple-observable"
                ),
                labels=[melf_key],
                key="Url.value",
                value=patter,
            )
            bundleobj.append(url_stix)
            indicator_url = Indicator(
                id=OpenCTIStix2Utils.generate_random_stix_id("indicator"),
                labels=[melf_key],
                pattern_type="stix",
                name=patter,
                pattern="[url:value = '"+patter+"']",
                custom_properties={
                    "x_opencti_main_observable_type": "Url"
                }
            )
            bundleobj.append(indicator_url)
            relation_url=Relationship(
                id=OpenCTIStix2Utils.generate_random_stix_id("relationship"),
                relationship_type="based-on",
                source_ref=indicator_url.id,
                target_ref=url_stix.id,
                allow_custom=True,
            )
            bundleobj.append(relation_url)

```

Infine, nella figura di sopra mostriamo solo una parte del codice che è stato utilizzato per sviluppare il connettore, per ogni IOC raccolto vengono creati:

- **Indicatore:** va a specificare in particolare campi come, il *pattern_type* posto come 'stix', il valore associato all'oggetto che si andrà a creare (*pattern*) e soprattutto una *custom_properties* che identificherà l'oggetto come di tipo 'Url'.
- **SimpleObservable:** viene creato principalmente per arricchire le informazioni di un determinato Observable utilizzando altri connettori di internal-enrichment. Si compone di campi come le *labels*, la *key* e il *value*.
- **Relationship:** serve per creare una relazione tra un Indicatore custom (*source_ref*) ed un SimpleObservable (*target_ref*).

8. Casi D'uso

8.4. CVE Trends

Il connettore CVE Trends realizzato si presenta nel seguente modo sulla piattaforma.

The screenshot shows the 'CVE TRENDS' connector interface. On the left, there's a sidebar with 'Activities' expanded, showing 'Analysis', 'Events', 'Observations', 'Knowledge', 'Threats', 'Arsenal', 'Entities', 'Data', and 'Settings'. The main area has a dark header 'CVE TRENDS ACTIVE'. Under 'BASIC INFORMATION', it shows 'Type: EXTERNAL_IMPORT', 'Last update: Feb 3, 2022, 5:24:39 PM', 'Only contextual: NOT APPLICAB...', 'Automatic trigger: NOT APPLICAB...', and 'Scope: Vulnerability'. In the 'IN PROGRESS WORKS' section, there's one entry: 'Name: Template run @ 2022-02-03 15:39:50', 'Status: IN PROGRESS', 'Operations completed: 0', 'Total number of operations: 11', and '0 ERRORS'.

Un esempio è quello di **CVE-2022-23601**, il connettore ha generato diverse informazioni a riguardo, come la *descrizione*, lo *score*, la *severity* e il *confidence level*.

The screenshot shows the details of the CVE-2022-23601 vulnerability. The left sidebar is identical to the previous screenshot. The main area has a dark header 'CVE-2022-23601'. Under 'BASIC INFORMATION', it shows 'Standard STIX ID: vulnerability--3a0531e6-c202-5510-8b29-16ffc490dc6d' and 'Other STIX IDs: -'. In the 'DETAILS' section, there's a large 'Description' block detailing a security issue in Symfony. It also shows 'CVSS3 - Score: 8.8', 'CVSS3 - Severity: HIGH', 'CVSS3 - Availability impact (A): Unknown', 'CVSS3 - Integrity impact (I): Unknown', 'CVSS3 - Confidentiality impact (C): Unknown', and 'CVSS3 - Attack vector (AV): Unknown'. A red edit icon is visible next to the CVSS3 - Attack vector (AV) field.

Altre informazioni importanti sono mantenute nella sezione degli EXTERNAL REFERENCES, qui sono presenti:

- Link al tweet che ha identificato la vulnerabilità
- NIST NVD, che contiene le informazioni riguardanti una CVE
- Link Reddit

- Link GitHub

8.2 UrlscanIo

Urlscan.io essendo un connettore di **Enrichment** può essere avviato manualmente o in automatico affinché ci sia l'analisi dell'*observable* considerato.

Una volta avviato, il connettore con una spunta verde indicherà l'effettiva analisi andata a buon fine.

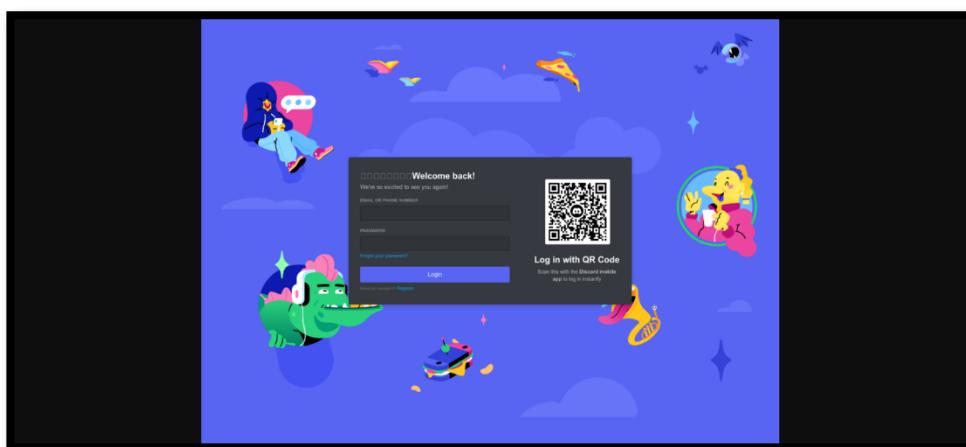
La pagina dell'***observable*** viene arricchita con i campi definiti nel codice del connettore .
In questo caso abbiamo quindi:

- Lo score

- Le label sull'origine del dominio (es: “de”, “us”)
- Le label di pericolo/segnalazione, ad esempio, come “*phishing*” (specifica del tipo di malware) e “*malicious*” (se malevolo)
- La sezione descrizione con i parametri messi a disposizione da Urlscan.io

Nella sezione degli *External References* vengono invece individuati i report e il live screenshot

Il report ci riporta a ciò che si può vedere se manualmente viene effettuata la ricerca dell'url su “<https://urlscan.io/>”



Il live screenshot invece presenta un’istantanea dell'url che permette di vedere in anteprima ciò che si sta analizzando.

8.3. IOCTweet

8.3.1 Caso d'uso hash file

Il connettore in questo caso ha analizzato un hash file di tipo 'SHA-256'. Come detto in precedenza viene preso il *value*, che corrisponde all'hash, una *label* che corrisponde al Malware. In basso è presente anche una relationship di tipo '*based-on*' per creare la relazione con il corrispettivo Observable

The screenshot shows a detailed view of a digital forensic or intelligence platform. At the top, the identifier '3B491E81086C7A723A259227D714505043801633ED78CE5785...' is displayed. The interface is divided into several sections:

- BASIC INFORMATION**:
 - Standard STIX ID: indicator--eb514046-5d93-5475-9fa8-1d60ae7ebfdf
 - Other STIX IDs: -
 - Pattern type: STIX
 - Author: -
 - Distribution of opinions: 5/5 (strongly-disagree to strongly-agree)
 - Confidence level: LOW
 - Creation date (in this platform): February 5, 2022, 12:23:31 AM
 - Creator: IOCTWEET
 - Creation date: February 5, 2022, 12:20:55 AM
- DETAILS**:
 - Indicator pattern: [file:hashes.'SHA-256' = '3b491e81086c7a723a259227d714505043801633ed78ce5785aa56fdf1f254f']
 - Valid from: FEBRUARY 5, 2022
 - Valid until: FEBRUARY 5, 2023
 - Score: 50 / 100
 - Detection: NO
 - Description: Kill chain phases
 - Indicator types: MALICIOUS-ACTIVITY
 - Platforms: -
 - Based on: + (File)
- LATEST CREATED RELATIONSHIPS**: based on File: 3b491e81086c7a723... None
- LATEST REPORTS ABOUT THIS ENTITY**: No entities of this type has been found.
- EXTERNAL REFERENCES**: No entities of this type has been found.
- MOST RECENT HISTORY**: + IOCTWEET creates a Indicator 3b49... Feb 5, 2022, 12:23:32 AM

Cliccando sull'Observable creato verrà mostrato l'oggetto di tipo SimpleObservable creato

The screenshot shows a detailed view of a SimpleObservable object. The left panel, titled 'BASIC INFORMATION', contains fields such as Standard STIX ID (file--9e63a50f-2e58-5279-bdf2-b9366f4b2020), Other STIX IDs (empty), Observable type (File), Labels (#formbook), Score (NULL / 100), STIX version (2.1), Author (empty), and a distribution of opinions chart. The right panel, titled 'DETAILS', shows fields like Description (empty), SHA-256 hash (3b491e81086c7a723a259227d714505043801633ED78CE5785...), Creator (IOCTWEET), Creation date (February 5, 2022, 12:23:30 AM), and Modification date (February 5, 2022, 10:31:49 AM).

8.3.2 Caso d'uso Url

The screenshot shows an Indicator object for the URL <https://csinoticias.com/wp-includes/RNHJIZG/>. The left sidebar shows the navigation menu. The main panel has two tabs: 'BASIC INFORMATION' and 'DETAILS'. In the 'BASIC INFORMATION' tab, fields include Standard STIX ID (Indicator--73085d0b-b38d-5f4c-9618-581b1420d77e), Other STIX IDs (empty), Pattern type (STIX), Revoked (NO), Author (empty), Distribution of opinions (strongly-disagree, disagree, neutral, agree, strongly-agree), Confidence level (LOW), and Creation date (February 4, 2022, 8:21:10 PM). In the 'DETAILS' tab, fields include Indicator pattern ([url:value = 'https://csinoticias.com/wp-includes/RNHJIZG/']), Valid from (FEBRUARY 4, 2022), Valid until (FEBRUARY 4, 2023), Score (50 / 100), Detection (NO), Description (Kill chain phases), Indicator types (MALICIOUS-ACTIVITY), Platforms (empty), and Based on (URL: https://csinoticias.com/wp-in... Feb 4, 2022). A red edit button is visible at the bottom right.



L'indicatore creato da **IOCTweet**, in questo caso riferito ad un **URL** viene arricchito con:

- Lo score
- L'indicator pattern necessario e dipendente dal tipo di *observable* considerato
- Le Label di appartenenza alla famiglia di malware specifici

Inoltre, sono presenti nella sezione **based-on** gli *observable* a cui esso è collegato

The screenshot shows the OpenCTI interface for an observable entity. The URL is <https://csinoticias.com/wp-includes/Rnhjizg/>. The basic information includes a Standard STIX ID (url--7a48f428-3286-5dad-a207-1ad81910a436), an Observable type (URL), Labels (#emotet, #redline), a Score of 0 / 100, a STIX version of 2.1, and a Creator (IOCTWEET). The details section shows the description "secure request2, secure percentage:100, IPv6 percentage:0, uniq countries:1, total links:2, adBlocker:0" and the value "https://csinoticias.com/wp-includes/Rnhjizg/". The timeline shows "LATEST CREATED RELATIONSHIPS" and "LATEST REPORTS ABOUT THIS ENTITY". A red edit icon is visible in the bottom right corner.

L'*observable* in questione, un URL, viene automaticamente sottoposto all'analisi di [urlscan.io](#), il secondo connettore considerato in precedenza che lo arricchisce con le informazioni apposite.

Nell'*observable* è presente quindi la **relationship** biunivoca con l'indicatore prima introdotto

The screenshot shows the OpenCTI interface for an observable entity. The URL is <https://csinoticias.co...>. The latest created relationship is "based on Indicator https://csinoticias.co... None". The external references section includes a "Screen Shot" from urlscan.io and a link to "Urllscan.io". The most recent history shows several events: "Urllscan.io adds Screen Shot in...", "Urllscan.io replaces secure req...", "Urllscan.io adds Urllscan.io in...", "Urllscan.io replaces @ in x_open...", "IOCTweet adds #emotet in labels", and "IOCTweet creates a Url https://c...". A red edit icon is visible in the bottom right corner.

urllscan.io Home Search Live API Blog Docs Pricing Login Sponsored by SecurityTrails

csinoticias.com
162.214.49.220

URL: <https://csinoticias.com/wp-includes/RnHjlzg/>
 Submission: On February 04 via api (February 4th 2022, 7:41:27 pm UTC) from IT — Scanned from IT

[Summary](#) [HTTP 2](#) [Redirects](#) [Links 2](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#)

Summary

This website contacted 3 IPs in 1 countries across 2 domains to perform 2 HTTP transactions. The main IP is 162.214.49.220, located in United States and belongs to UNIFIEDLAYER-AS-1, US. The main domain is csinoticias.com.
 TLS certificate: Issued by R3 on January 28th 2022. Valid for: 3 months.

[csinoticias.com](#) scanned 6 times on urllscan.io [Show Scans 6](#)

urllscan.io Verdict: No classification

Live information

Google Safe Browsing: Malicious for csinoticias.com
 Current DNS A record: 162.214.49.220 (AS46606 - UNIFIEDLAYER-AS-1, US)
 Domain created: August 7th 2019, 17:33:20 (UTC)
 Domain registrar: GoDaddy.com, LLC

Screenshot

Please install flash player Pro to view the page (choose):
 • Flash Player 11.0.102.400
 • Google Flash Player
 • Microsoft Silverlight
 • Java Applet
 • PDF Reader
 • PDF.js
 • PDF.js Lite
 Updating Take a few seconds and no internet connection after installation.
[UPDATE](#) [RETRY](#)

Detected technologies

[WordPress \(CMS\)](#) [Expand](#)

Page Statistics

2	100 %	0 %	2	2
---	-------	-----	---	---

Urllscan.io quindi, fornisce negli *external reference* dell'*Observable* creato da **IOCTweet** il *report* e il *live screenshot* della pagina dell'URL dando quindi la possibilità ai due connettori di essere funzionali e cooperativi allo stesso tempo.

Esportazione IOC per IOCTweet

Nella sezione degli Indicator è possibile individuare, sfruttando la ricerca tramite labels, la lista di tutti gli IOC considerati per lo specifico Malware, individuandone il pattern, il nome e la data di creazione.

The screenshot shows the OpenCTI Cyber Threat Intelligence platform interface. The left sidebar contains navigation links for Dashboard, Activities, Analysis, Events, Observations, Knowledge, Threats, Arsenal, Entities, Data, and Settings. The main area displays a list of indicators. At the top of the list is an indicator labeled '#formbook' with a creation date of Feb 10, 2022, and a valid until date of Feb 10, 2023. Below this, there are 104 other entities. To the right of the list, there are sections for 'Indicator type' (listing STIX, PCRE, SIGMA, SNORT, Suricata, YARA, and Tanium Signal) and 'Observable type' (listing Artifact, Autonomous System, Cryptocurrency wallet, and others). A red circle with a plus sign is located at the bottom right of the indicator list. The status bar at the bottom right shows the date as 10/02/2022 and the time as 19:40.

Nella sezione di Exports List è possibile esportare ad esempio in un file csv, la lista di IOC con le relative informazioni, che la piattaforma mette a disposizione.

The screenshot shows the OpenCTI Cyber Threat Intelligence platform interface. On the left, there's a sidebar with navigation links: Dashboard, Activities, Analysis, Events, Observations, Knowledge, Threats, Arsenal, Entities, Data, and Settings. The main area displays a table of indicators. Each indicator row contains a checkbox, a pattern type icon, a name, labels (e.g., #formbook), creation date, valid until date, and a marking icon. A modal dialog box is open over the table, titled "Apertura di 2022-02-10T10:21:28.763Z_TLP_J", with the message: "È stato scelto di aprire: ...-2>1 21 28.763Z_TLP_J_(ExportFileCsv)_Indicator_full.csv". It includes options to "Apri con LibreOffice (predefinita)" or "Salva file", and a checkbox for "D'ora in poi eseguire questa azione per tutti i file di questo tipo". At the bottom right of the table, there's a red circular button with a plus sign. To the right of the table, there are sections for "Indicator type" (STIX, PCRE, SIGMA, SNORT, Suricata, YARA, Tanium Signal) and "Exports list" (a table of recent exports with columns for date, file name, and status). The bottom of the screen shows the Windows taskbar with various pinned icons.

Gli IOC vengono quindi esportati in un file come quello sottostante, in maniera tale da permetterne lo studio anche al di fuori della piattaforma.

Conclusioni

OpenCTI è una piattaforma per archiviare e gestire la Cyber Threat Intelligence per un'organizzazione. È molto utile in quanto automatizza molte operazioni che spesso vengono fatte manualmente.

L'installazione dei connettori, già implementati dal team di OpenCTI, ha richiesto diversi passaggi, i quali sono ben descritti nella documentazione. Inoltre, per mantenere sempre aggiornate le chiavi e i token di accesso all'interno dei diversi docker-compose che compongono i connettori è stato utilizzato un unico stack che li raggruppa; tutto ciò ci è stato permesso dalla piattaforma di Portainer.

Infine, per testare la piattaforma sono stati implementati altri tre connettori custom (CveTrends, UrlScanlo e IOCTweet), ciò ci ha aiutato a comprendere meglio quale fosse il meccanismo e il processo implementativo che si trova dietro un connettore. L'esperienza ottenuta dallo studio e dall'implementazione dei connettori della piattaforma OpenCTI ci ha introdotto nel mondo relativamente nuovo della Cyber Threat Intelligence.