



Università Degli Studi Del Sannio

Dipartimento di Ingegneria

Corso di Laurea Magistrale in Ingegneria Informatica

Anno Accademico 2021/2022

Documentazione

Security Affairs Connector

Malware Bazaar Connector

Bleeping Computer Connector

Talos Intelligence Connector

Docente del corso:

Corrado Aaron Visaggio

Assistente del corso:

Pietro Melillo

Gruppo UNICS:

Cavoto Pasquale

Bosco Matteo

Crisci Raffaella

Ungolo Pio Augusto

INDICE

1. OpenCTI Platform	5
1.1 Introduzione	5
1.2 STIX2	7
2. Security Affairs	9
2.1 Introduzione	9
2.2 Installazione Connettore	9
2.2.1 Requisiti	9
2.2.2 Requisiti	9
2.2.2.1 Standalone Python Process	9
2.2.2.2 Docker Compose Process	9
2.2.2.2 Portainer Process	9
2.2.3 Requisiti	9
2.3 Analisi e raccolta dati	11
2.3.1 Report	11
2.3.2 AttackPattern	11
2.3.3 Identity	11
2.3.4 ExternalReference	11
2.4 Creazione bundle (stix2)	11
3. Bleeping Computer	12
3.1 Introduzione	12
3.2 Installazione Connettore	12
3.2.1 Requisiti	12
3.2.2 Requisiti	12
3.2.2.1 Standalone Python Process	12
3.2.2.2 Docker Compose Process	12
3.2.2.2 Portainer Process	12
3.2.3 Requisiti	12
3.3 Analisi e raccolta dati	13
3.3.1 Report	14
3.3.2 Malware	14
3.3.3 Identity	14

3.3.4 Note	14
3.3.5 ExternalReference	14
3.4 Creazione bundle (stix2)	14
4. Talos Intelligence	15
4.1 Introduzione	15
4.2 Installazione Connettore	15
4.2.1 Requisiti	15
4.2.2 Requisiti	15
4.2.2.1 Standalone Python Process	15
4.2.2.2 Docker Compose Process	15
4.2.2.2 Portainer Process	15
4.2.3 Requisiti	15
4.3 Analisi e raccolta dati	16
4.3.1 Report	17
4.3.2 Relationship	17
4.3.4 Vulnerability	17
4.3.5 Note	17
4.3.6 ExternalReference	18
4.4 Creazione bundle (stix2)	18
5. Malware Bazaar	19
5.1 Introduzione	19
5.2 Installazione Connettore	19
5.2.1 Requisiti	19
5.2.2 Requisiti	19
5.2.2.1 Standalone Python Process	19
5.2.2.2 Docker Compose Process	19
5.2.2.2 Portainer Process	19
5.2.3 Requisiti	19
5.2 Analisi e raccolta dati	20
5.3.1 Report	25
5.3.2 Relationship	25
5.3.4 Indicator	25
5.3.5 Note	25

5.3.6 ExternalReference	25
5.3.7 Malware	26
5.4 Creazione bundle (stix2)	26
6. Casi d'uso	27
6.1 Ricerca IOC riguardo la vulnerabilità 'log4shell' di log4j	27
6.2 Ricerca IOC riguardo 'CVE-2021'	27
6.3 Export IOC	29
6.4 Ricerca IOC riguardo 'CVE-2021-1384'	31

1. OpenCTI Platform

1.1 Introduzione

<https://www.opencti.io/en/>

OpenCTI è una piattaforma *Open Source* che consente alle organizzazioni di gestire la loro conoscenza degli *Observables* (file, documentazione, etc...) riguardanti la *Cyber Threat Intelligence*. E' stata creata per strutturare, organizzare, conservare e visualizzare le informazioni tecniche e non-tecniche riguardanti le *Cyber threats*.

I dati sono strutturati utilizzando un *Knowledge Schema* basato sullo standard *STIX2*. La piattaforma è stata realizzata come una moderna web application che include *GraphQL API* e un frontend *UX Oriented*. OpenCTI può essere integrato con altri tool e applicazioni come *MISP*, *TheHive*, *MITRE ATT&CK*, etc.

L'obiettivo della piattaforma è quello di creare un tool comprensivo che consenta agli utenti di integrare le informazioni tecniche (come i TTPs e gli observables) e le informazioni non-tecniche (come vittimologia, settore di attività e localizzazione), collegando ogni informazione alla propria fonte e consentendo di collegare tra loro le informazioni in base ai campi che le descrivono.

All'interno della piattaforma troviamo le seguenti sezioni:

- Dashboard: sezione principale, dove è possibile visualizzare i dati in tempo reale appena caricati
- Activities:
 - Analysis
 - Reports
 - Notes
 - Opinions
 - External References
 - Events
 - Observation
 - Observables
 - Artifacts
 - Indicators
 - Infrastructures
- Knowledge
 - Threats
 - Malwares
 - Attack patterns
 - Course of action
 - Tools
 - Vulnerabilities
 - Arsenal
 - Sectors
 - Countries

- Cities
 - Positions
 - Organizations
 - Systems
 - Individuals
- Entities
- Data
 - Entities
 - Background tasks
 - Connectors
 - Synchronization
 - Data sharing
 - TAXII collections
- Settings
 - Parameters
 - Access
 - Roles
 - Users
 - Groups
 - Marking definitions
 - Sessions
 - Workflows
 - Retention policies
 - Rules

1.2 STIX2

<https://oasis-open.github.io/cti-documentation/stix/intro.html>

[oasis-open/cti-python-stix2](https://github.com/oasis-open/cti-python-stix2): OASIS TC Open Repository: Python APIs for STIX 2 (github.com)

Structured Threat Information Expression (STIX) è un linguaggio e un formato di serializzazione *Open Source* utilizzato per scambiare *Cyber Threat Intelligence (CTI)*.

STIX consente di descrivere i CTI tramite degli oggetti che consentono di categorizzare le informazioni attraverso degli attributi. Le informazioni possono essere correlate tra loro tramite la creazione di relazioni che consentono di rappresentare CTI complessi come insieme di più oggetti STIX.

Gli oggetti definiti in STIX2 sono:

- *Attack Pattern*:
 - Un tipo di TTP che descrive i modi con cui un adversary cerca di compromettere un target.
- *Campaign*:
 - Un raggruppamento di comportamenti degli adversary che descrive un insieme di attività o attacchi malevoli eseguiti contro un target specifico in un determinato intervallo di tempo.
- *Course of Action*:
 - Una raccomandazione dal produttore al consumatore riguardo le azioni da intraprendere in risposta alle informazioni di Cyber Threat ricevute.
- *Grouping*:
 - Definisce in modo esplicito il contesto di un insieme di oggetti STIX.
- *Identity*:
 - Un individuo, organizzazione o gruppo legato all'informazione di Cyber Threat.
- *Indicator*:
 - Specifica un pattern che può essere utilizzato per individuare attività informatiche sospette o malevole.
- *Infrastructure*:
 - Rappresenta un tipo di TTP che descrive sistemi, servizi software e risorse fisiche o virtuali associate, che vengono utilizzate per eseguire un attacco o che vengono attaccate.
- *Intrusion Set*:
 - Un raggruppamento di comportamenti degli adversary e delle risorse che hanno proprietà comuni e che si crede siano gestite da una singola organizzazione.
- *Location*:
 - Rappresenta una locazione geografica.
- *Malware*:
 - Un tipo di TTP che rappresenta del codice malevolo.
- *Malware Analysis*:
 - Metadata e risultati di una particolare analisi (statica o dinamica) su un'istanza o una famiglia di malware.
- *Note*:
 - Contiene testo informativo e fornisce informazioni aggiuntive non presenti all'interno di un oggetto STIX.
- *Observed Data*:

- Contiene informazioni riguardo entità legate alla Cyber Security come file, sistemi, network ecc.
- *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, ad esempio una descrizione di un attore di minacce, malware o tecnica di attacco, inclusi contesto e dettagli correlati.
- *Threat Actor:*
 - Individui, gruppi o organizzazioni reali che si ritiene operino con intenti dannosi.
- *Tool:*
 - Software legittimo che può essere utilizzato dagli attori delle minacce per eseguire attacchi.
- *Vulnerability:*
 - Un errore nel software che può essere utilizzato direttamente da un hacker per accedere a un sistema oa una rete.

Le relazioni definite da STIX2 sono:

- *Relationship:*
 - Utilizzato per collegare due oggetti STIX per descrivere come sono correlati tra loro.
- *Sighting:*
 - Denota la convinzione che qualcosa in CTI (ad esempio, un indicator, malware, tool, threat actor, ecc.) sia stato visto.

2. Security Affairs

2.1 Introduzione

<https://securityaffairs.co/wordpress/>

Pierluigi Paganini, fondatore di Security Affairs, CYBHORUS e Cybaze SpA. una delle principali realtà italiane in cyber security Membro del gruppo di lavoro ad-hoc sui paesaggi delle minacce informatiche.

Perché è stato scelto?

Il suo blog Security Affairs è considerato uno dei primi 5 al mondo in materia, inoltre quotidianamente pubblica vari articoli aggiornati riguardo l'attualità della cyber security.

2.2 Installazione Connettore

2.2.1 Requisiti

Per l'installazione del connettore è necessario utilizzare la versione 5.0.3 (o superiore) della piattaforma OpenCTI. Il modo migliore per installare il connettore è utilizzare la Dashboard di Portainer, ma è possibile installare il connettore tramite Docker Compose ed eseguirlo con Python.

Il connettore necessita dell'accesso alla piattaforma tramite OpenCTI Connector Token (ottenibile tramite la creazione di un nuovo utente, e all'istanza di RabbitMQ in esecuzione sul sistema su cui è installata la piattaforma.

2.2.2 Requisiti

2.2.2.1 Standalone Python Process

Per configurare il connettore è necessario utilizzare il file *config.yml*. Le librerie Python necessarie per l'installazione del connettore devono essere specificate nel file *requirements.txt* e devono essere installate tramite il comando *pip3 install -r requirements.txt -U*. Per eseguire il connettore in Detached mode bisogna utilizzare il comando *python3 main.py &* all'interno della directory in cui è presente il file *main.py* del connettore.

2.2.2.2 Docker Compose Process

Per configurare il connettore è necessario utilizzare il file *docker-compose.yml*. Per caricare il connettore sulla piattaforma ed eseguirlo è necessario eseguire il comando *docker-compose up* all'interno della directory in cui è presente il file di configurazione.

2.2.2.2 Portainer Process

Per configurare il connettore è necessario specificare la corretta configurazione nello *stack* della Dashboard di Portainer. Per caricare ed eseguire il connettore basta premere il pulsante *Update the stack* presente nell'interfaccia di Portainer.

2.2.3 Requisiti

Di seguito è riportata la tabella con i parametri di configurazione per il caricamento e l'esecuzione del connettore tramite Docker o Portainer.

Docker envvar	Parameter	Default	Description
OPENCTI_URL	opencti_url	http://opencti:8080	The URL of the OpenCTI platform.
OPENCTI_TOKEN	opencti_token	changeMe	The user token provided in the OpenCTI platform.
CONNECTOR_ID	connector_id	changeMe	A valid arbitrary <code>UUIDv4</code> that must be unique for this connector.
CONNECTOR_TYPE	connector_type	EXTERNAL_IMPORT	Must be <code>EXTERNAL_IMPORT</code> (this is the connector type).
CONNECTOR_NAME	connector_name	SecurityAffairs	Option <code>SecurityAffairs</code>
CONNECTOR_SCOPE	connector_scope	Bundle, Malware, Report, Note, Relationship, Identity, ExternalReference	Supported scope: Template Scope (MIME Type or Stix Object)
CONNECTOR_CONFIDENCE_LEVEL	connector_confidence_level	100	The default confidence level for created sightings (a number between 0 and 100).
CONNECTOR_LOG_LEVEL	connector_log_level	info	The log level for this connector, could be <code>debug</code> , <code>info</code> , <code>warn</code> or <code>error</code> (less verbose).
SECURITYAFFAIRS_INTERVAL	securityaffairs_interval	2	Must be strictly greater than 1, indicates the frequency of update in days (default value is 2 days).

2.3 Analisi e raccolta dati

Analizzando il sito si evince che è principalmente un blog. Per prelevare i dati da un blog è possibile operare lo scraping della pagina html oppure fare richiesta ai feed RSS.

Struttura feed: gli articoli sono divisi in items, per ogni items abbiamo:

- title (titolo articolo)
- creator (autore)
- description (corpo articolo)
- pubData (data di pubblicazione)
- category (categoria)

Il pacchetto in formato json recuperato incorpora i campi citati e filtrati. Da questo pacchetto è stato possibile creare i seguenti oggetti in formato STIX2:

2.3.1 Report

PROPERTY	REQUIRED	TYPE
report_types		REPORT_TYPE
description		String
name	YES	String
labels		List(String)
created_by_ref		Reference(Identity)
published	YES	TimeStamp
object_refs	YES	List(Reference(SDO))
external_references		List(ExternalReference)

2.3.2 AttackPattern

PROPERTY	REQUIRED	TYPE
name	YES	String
description		String

2.3.3 Identity

PROPERTY	REQUIRED	TYPE
name	YES	String
external_references		List(ExternalReference)

2.3.4 ExternalReference

PROPERTY	REQUIRED	TYPE
url		String
description		String
source_name	YES	String

2.4 Creazione bundle (stix2)

I bundle sono stati creati con Identity, AttackPattern e Report relazionati tra di loro.

Identity	AttackPattern	Report
----------	---------------	--------

3. Bleeping Computer

3.1 Introduzione

Bleeping Computer è un sito Web che copre le notizie di tecnologia e offre assistenza informatica gratuita tramite i suoi forum, creato da Lawrence Abrams nel 2004.

Pubblica notizie concentrandosi molto sulla sicurezza informatica, ma copre anche altri argomenti, tra cui software , hardware , operativo sistema e tecnologia generale.

<https://www.bleepingcomputer.com/>

3.2 Installazione Connettore

3.2.1 Requisiti

Per l'installazione del connettore è necessario utilizzare la versione 5.0.3 (o superiore) della piattaforma OpenCTI. Il modo migliore per installare il connettore è utilizzare la Dashboard di Portainer, ma è possibile installare il connettore tramite Docker Compose ed eseguirlo con Python.

Il connettore necessita dell'accesso alla piattaforma tramite OpenCTI Connector Token (ottenibile tramite la creazione di un nuovo utente, e all'istanza di RabbitMQ in esecuzione sul sistema su cui è installata la piattaforma.

3.2.2 Requisiti

3.2.2.1 Standalone Python Process

Per configurare il connettore è necessario utilizzare il file *config.yml*. Le librerie Python necessarie per l'installazione del connettore devono essere specificate nel file *requirements.txt* e devono essere installate tramite il comando `pip3 install -r requirements.txt -U`. Per eseguire il connettore in Detached mode bisogna utilizzare il comando `python3 main.py &` all'interno della directory in cui è presente il file *main.py* del connettore.

3.2.2.2 Docker Compose Process

Per configurare il connettore è necessario utilizzare il file *docker-compose.yml*. Per caricare il connettore sulla piattaforma ed eseguirlo è necessario eseguire il comando `docker-compose up` all'interno della directory in cui è presente il file di configurazione.

3.2.2.2 Portainer Process

Per configurare il connettore è necessario specificare la corretta configurazione nello *stack* della Dashboard di Portainer. Per caricare ed eseguire il connettore basta premere il pulsante *Update the stack* presente nell'interfaccia di Portainer.

3.2.3 Requisiti

Di seguito è riportata la tabella con i parametri di configurazione per il caricamento e l'esecuzione del connettore tramite Docker o Portainer.

Docker envvar	Parameter	Default	Description
OPENCTI_URL	opencti_url	http://opencti:8080	The URL of the OpenCTI platform.
OPENCTI_TOKEN	opencti_token	changeMe	The user token provided in the OpenCTI platform.
CONNECTOR_ID	connector_id	changeMe	A valid arbitrary <code>UUIDv4</code> that must be unique for this connector.
CONNECTOR_TYPE	connector_type	EXTERNAL_IMPORT	Must be <code>EXTERNAL_IMPORT</code> (this is the connector type).
CONNECTOR_NAME	connector_name	BleepingComputer	Option <code>BleepingComputer</code>
CONNECTOR_SCOPE	connector_scope	Bundle, Malware, Report, Note, Relationship, Identity, ExternalReference	Supported scope: Template Scope (MIME Type or Stix Object)
CONNECTOR_CONFIDENCE_LEVEL	connector_confidence_level	100	The default confidence level for created sightings (a number between 0 and 100).
CONNECTOR_LOG_LEVEL	connector_log_level	info	The log level for this connector, could be <code>debug</code> , <code>info</code> , <code>warn</code> or <code>error</code> (less verbose).
BLEEPING_INTERVAL	bleeping_interval	2	Must be strictly greater than 1, indicates the frequency of update in days (default value is 2 days).

3.3 Analisi e raccolta dati

Le informazioni sono state estratte dal feed RSS di BleepingComputer.

Le informazioni contenute erano principalmente relative a Malware. Principalmente i feed contengono:

- Nome del Malware;
- Descrizione breve del Malware;

- [Link alla descrizione completa del Malware.](#)

Di seguito sono riportati gli STIX Object utilizzati per descrivere le informazioni estratte dal connettore:

3.3.1 Report

PROPERTY	REQUIRED	TYPE
report_types		REPORT_TYPE
description		String
name	YES	String
labels		List(String)
created_by_ref		Reference(Identity)
published	YES	TimeStamp
object_refs	YES	List(Reference(SDO))
external_references		List(ExternalReference)

3.3.2 Malware

PROPERTY	REQUIRED	TYPE
is_familiy	YES	Boolean
name		String
description		String
labels		String
external_references		List(ExternalReference)

3.3.3 Identity

PROPERTY	REQUIRED	TYPE
name	YES	String
external_references		List(ExternalReference)

3.3.4 Note

PROPERTY	REQUIRED	TYPE
content	YES	String
object_refs	YES	List(Reference(SDO))
labels		String
external_references		List(ExternalReference)

3.3.5 ExternalReference

PROPERTY	REQUIRED	TYPE
url		String
description		String
source_name	YES	String

3.4 Creazione bundle (stix2)

I bundle sono stati creati con Identity, Malware, Report, Note e relazionati tra di loro.

Identity	Malware	Report	Note
----------	---------	--------	------

4. Talos Intelligence

4.1 Introduzione

Cisco Talos è uno dei più grandi team commerciali di intelligence sulle minacce al mondo, composto da ricercatori, analisti e ingegneri di livello mondiale. La visibilità leader del settore, l'intelligence azionabile e la ricerca sulle vulnerabilità guidano il rilevamento rapido e la protezione per i clienti Cisco contro le minacce note ed emergenti e fermano le minacce in libertà per proteggere Internet in generale.

<https://talosintelligence.com/>

4.2 Installazione Connettore

4.2.1 Requisiti

Per l'installazione del connettore è necessario utilizzare la versione 5.0.3 (o superiore) della piattaforma OpenCTI. Il modo migliore per installare il connettore è utilizzare la Dashboard di Portainer, ma è possibile installare il connettore tramite Docker Compose ed eseguirlo con Python.

Il connettore necessita dell'accesso alla piattaforma tramite OpenCTI Connector Token (ottenibile tramite la creazione di un nuovo utente, e all'istanza di RabbitMQ in esecuzione sul sistema su cui è installata la piattaforma.

4.2.2 Requisiti

4.2.2.1 Standalone Python Process

Per configurare il connettore è necessario utilizzare il file *config.yml*. Le librerie Python necessarie per l'installazione del connettore devono essere specificate nel file *requirements.txt* e devono essere installate tramite il comando *pip3 install -r requirements.txt -U*. Per eseguire il connettore in Detached mode bisogna utilizzare il comando *python3 main.py &* all'interno della directory in cui è presente il file *main.py* del connettore.

4.2.2.2 Docker Compose Process

Per configurare il connettore è necessario utilizzare il file *docker-compose.yml*. Per caricare il connettore sulla piattaforma ed eseguirlo è necessario eseguire il comando *docker-compose up* all'interno della directory in cui è presente il file di configurazione.

4.2.2.2 Portainer Process

Per configurare il connettore è necessario specificare la corretta configurazione nello *stack* della Dashboard di Portainer. Per caricare ed eseguire il connettore basta premere il pulsante *Update the stack* presente nell'interfaccia di Portainer.

4.2.3 Requisiti

Di seguito è riportata la tabella con i parametri di configurazione per il caricamento e l'esecuzione del connettore tramite Docker o Portainer.

Docker envvar	Parameter	Default	Description
OPENCTI_URL	opencti_url	http://opencti:8080	The URL of the OpenCTI platform.
OPENCTI_TOKEN	opencti_token	changeMe	The user token provided in the OpenCTI platform.
CONNECTOR_ID	connector_id	changeMe	A valid arbitrary <code>UUIDv4</code> that must be unique for this connector.
CONNECTOR_TYPE	connector_type	EXTERNAL_IMPORT	Must be <code>EXTERNAL_IMPORT</code> (this is the connector type).
CONNECTOR_NAME	connector_name	TalosIntelligence	Option <code>TalosIntelligence</code>
CONNECTOR_SCOPE	connector_scope	Bundle, Malware, Report, Note, Relationship, Identity, ExternalReference	Supported scope: Template Scope (MIME Type or Stix Object)
CONNECTOR_CONFIDENCE_LEVEL	connector_confidence_level	100	The default confidence level for created sightings (a number between 0 and 100).
CONNECTOR_LOG_LEVEL	connector_log_level	info	The log level for this connector, could be <code>debug</code> , <code>info</code> , <code>warn</code> or <code>error</code> (less verbose).
TALOS_INTERVAL	talos_interval	2	Must be strictly greater than 1, indicates the frequency of update in days (default value is 2 days).

4.3 Analisi e raccolta dati

Le informazioni sono state estratte tramite *Scraping* dalla pagina di Talos Intelligence. Le informazioni estratte riguardano principalmente:

- Vulnerabilità Zero Day;
- Vulnerabilità Disclosed.

Per le vulnerabilità Zero Day sono state estratte le seguenti informazioni:

- Talos Id (identificatore usato da talos per gestire le vulnerabilità);
- Data di pubblicazione.

Per le vulnerabilità Disclosed sono state estratte le seguenti informazioni:

- Talos Id;
- Codice CVE della vulnerabilità;
- Descrizione;
- Product Url (Link al sito del software interessato dalla vulnerabilità);
- Data di pubblicazione;
- Azioni eseguite dal Vendor del software interessato (come patch e update del software);
- Score CVSS della vulnerabilità.

Di seguito sono riportati gli STIX Object utilizzati per descrivere le informazioni estratte dal connettore:

4.3.1 Report

PROPERTY	REQUIRED	TYPE
report_types		REPORT_TYPE
description		String
name	YES	String
labels		List(String)
created_by_ref		Reference(Identity)
published	YES	TimeStamp
object_refs	YES	List(Reference(SDO))
external_references		List(ExternalReference)

4.3.2 Relationship

PROPERTY	REQUIRED	TYPE
relationship_type	YES	String
source_ref		Reference(SOURCE_REF)
target_ref		Reference(TARGET_REF)
confidence		Integer

4.3.3 Identity

PROPERTY	REQUIRED	TYPE
name	YES	String

4.3.4 Vulnerability

PROPERTY	REQUIRED	TYPE
name	YES	String
created		TimeStamp
description		String
labels		String
created_by_ref		Reference(Identity)
external_references		List(ExternalReference)

4.3.5 Note

PROPERTY	REQUIRED	TYPE
----------	----------	------

content	YES	String
object_refs	YES	List(Reference(SDO))
labels		String
external_references		List(ExternalReference)
abstract		String

4.3.6 ExternalReference

PROPERTY	REQUIRED	TYPE
url		String
description		String
source_name	YES	String

4.4 Creazione bundle (stix2)

Per questo connettore sono stati realizzati 2 bundle (uno per le vulnerability Zero Day e uno per le vulnerability Disclosed) così composti:

Disclosed Bundle:

Identity	Vulnerability	Note	Report	Relationship
----------	---------------	------	--------	--------------

Zero Day Bundle:

Identity	Vulnerability
----------	---------------

5. Malware Bazaar

5.1 Introduzione

MalwareBazaar è un progetto di abuse.ch con l'obiettivo di condividere campioni di malware con la comunità infosec, i fornitori di AV e i fornitori di informazioni sulle minacce.

Spesso i campioni di malware presenti in blog e altro non sono facilmente accessibili. Per evitare registrazioni e download è stato creato Malware Bazaar in cui i ricercatori di sicurezza IT possono condividere facilmente campioni di malware con la comunità senza incorrere in restrizioni di download per tutto il tempo o dover pagare costose quote di abbonamento.

<https://bazaar.abuse.ch/>

5.2 Installazione Connettore

5.2.1 Requisiti

Per l'installazione del connettore è necessario utilizzare la versione 5.0.3 (o superiore) della piattaforma OpenCTI. Il modo migliore per installare il connettore è utilizzare la Dashboard di Portainer, ma è possibile installare il connettore tramite Docker Compose ed eseguirlo con Python.

Il connettore necessita dell'accesso alla piattaforma tramite OpenCTI Connector Token (ottenibile tramite la creazione di un nuovo utente, e all'istanza di RabbitMQ in esecuzione sul sistema su cui è installata la piattaforma.

5.2.2 Requisiti

5.2.2.1 Standalone Python Process

Per configurare il connettore è necessario utilizzare il file *config.yml*. Le librerie Python necessarie per l'installazione del connettore devono essere specificate nel file *requirements.txt* e devono essere installate tramite il comando *pip3 install -r requirements.txt -U*. Per eseguire il connettore in Detached mode bisogna utilizzare il comando *python3 main.py &* all'interno della directory in cui è presente il file *main.py* del connettore.

5.2.2.2 Docker Compose Process

Per configurare il connettore è necessario utilizzare il file *docker-compose.yml*. Per caricare il connettore sulla piattaforma ed eseguirlo è necessario eseguire il comando *docker-compose up* all'interno della directory in cui è presente il file di configurazione.

5.2.2.2 Portainer Process

Per configurare il connettore è necessario specificare la corretta configurazione nello *stack* della Dashboard di Portainer. Per caricare ed eseguire il connettore basta premere il pulsante *Update the stack* presente nell'interfaccia di Portainer.

5.2.3 Requisiti

Di seguito è riportata la tabella con i parametri di configurazione per il caricamento e l'esecuzione del connettore tramite Docker o Portainer.

Docker envvar	Parameter	Default	Description
OPENCTI_URL	opencti_url	http://opencti:8080	The URL of the OpenCTI platform.
OPENCTI_TOKEN	opencti_token	changeMe	The user token provided in the OpenCTI platform.
CONNECTOR_ID	connector_id	changeMe	A valid arbitrary <code>UUIDv4</code> that must be unique for this connector.
CONNECTOR_TYPE	connector_type	INTERNAL_ENRICHMENT	Must be <code>INTERNAL_ENRICHMENT</code> (this is the connector type).
CONNECTOR_NAME	connector_name	MalwareBazaar	Option <code>MalwareBazaar</code>
CONNECTOR_SCOPE	connector_scope	Artifact, StixFile	Supported scope: Template Scope (MIME Type or Stix Object)
CONNECTOR_CONFIDENCE_LEVEL	connector_confidence_level	100	The default confidence level for created sightings (a number between 0 and 100).
CONNECTOR_AUTO	connector_auto	true	Connector needs the automatic trigger
CONNECTOR_LOG_LEVEL	connector_log_level	info	The log level for this connector, could be <code>debug</code> , <code>info</code> , <code>warn</code> or <code>error</code> (less verbose).
MALWAREBAZAAR_API_KEY	malwarebazaar_api_key	changeMe	Must be strictly greater than 1, indicates the frequency of update in days (default value is 2 days).
MALWAREBAZAAR_MAX_TLP	malwarebazaar_max_tlp	TLP:AMBER	

5.2 Analisi e raccolta dati

Malware bazaar fornisce un API per accedere alle informazioni presenti nel loro database. Per poter aggiornare le informazioni è necessario possedere un API Key ottenuta registrandosi alla piattaforma.

Le informazioni estratte da Malware Bazaar sono principalmente correlate a Malware.

Per richiedere un Malware sample è necessario utilizzare l'Hash del malware che si intende ricercare (il formato dell'hash può essere SHA256, MD5 o SHA1) tramite la richiesta *Query Sample*.

Key	Example	Comment
query	get_file	
sha256_hash	094fd325049b8a9cf6d3e5ef2a6d4cc6a567d7d49c35f8bb8dd9e3c6acf3d78d	SHA256 hash of the malware sample you want to download

Di seguito è riportata un esempio delle informazioni estratte tramite richiesta all'API:

Key	Value	Comment
query_status	http_post_expected	The API expected a HTTP POST request
	hash_not_found	The file (hash) you wanted to query is unknown to MalwareBazaar
	illegal_hash	The hash you provided is not a valid SHA256 hash
	no_hash_provided	You did not provide a hash
sha256_hash	e167b20f1acf48f7ce0ae33a218e...	SHA256 hash of the malware sample
sha3_384_hash	19142fcef2eb63b4a000506d81218...	SHA3-384 hash of the malware sample
sha1_hash	eb0e81598d8526d88cac4695a3e9360cc8fbb331	SHA1 hash of the malware sample
md5_hash	7338b335ad5471cb67658f27836374f0	MD5 hash of the malware sample
first_seen	2020-02-28 05:57:01	TS when the file has been first seen by MalwareBazaar (UTC)

last_seen	2020-03-01 08:11:45	TS when the file has been last seen by MalwareBazaar (UTC)
file_name	Jamil Marzouka Co.pdf.jar	Malware sample's file name
file_size	62118	File size in bytes
file_type_mime	application/x-dosexec	MIME file type
file_type	jar	File type
reporter	viql	Twitter handle of the report (or anonymous for anonymous submissions)
origin_country	US	Two letter country code of the country where the sample was uploaded from
anonymous	0	1 (true) or 0 (false)
signature	Adwind	Malware family (if available)
imphash	f34d5f2d4577ed6d9ceec516c1f5a744	imphash (only available for PE executables)
tlsh	11B2194E3FA98856C4BC177486B...	Trend Micro Locality Sensitive Hash (tlsh)
telfhash	1E634BC4B643D9F2ED0602B52477EF338E76F5B...	Trend Micro ELF Hash (telfhash)
ssdeep	1536:sGZWpdxayQAcj7gwluW14Z2II0oc...	ssdeep
dhash_icon	f8dcbeffbffecee8	In case the file is a PE executable: dhash of the samples icon
tags	Adwind, jar, qua	list of tags
code_sign	subject_cn	Subject Common Name (CN)
	issuer_cn	Issuer Common Name (CN)
	algorithm	Algorithm used

	valid_from	Datetime valid from
	valid_to	Datetime valid to (expire date)
	serial_number	Serial number
	cscb_listed	Code Signing Certificate Blocklist (CSCB) status (True or False)
	cscb_reason	Code Signing Certificate Blocklist (CSCB) listing reason
delivery_method	email_attachment	Distributed via e-mail attachment
	email_link	Distributed via e-mail link
	web_download	Distributed via web download
	web_drive-by	Distributed via drive-by
	multiple	Multiple delivery methods used
	other	Other delivery methods used
file_information	various	Contextual information about the file sample
yara_rules	rule_name	Name of the YARA rule that triggered
	author	Author of the YARA rule
	description	Description of the YARA rule
	reference	Reference of the YARA rule
ole_information	oleid	Results from oleid
	olevba	Results from olevba
vendor_intel	ANY.RUN	Dynamic malware analysis from ANY.RUN

	CAPE	Dynamic malware analysis from CAPE Sandbox
	CERT-PL_MWDB	Threat intel from CERT.PL Malware Database
	vxCube	Dynamic malware analysis from Dr.Web vxCube
	DocGuard	Office document reputation from DocGuad
	FileScan-IO	Malware analysis service from FileScan.IO
	InQuest Labs	File reputation service from InQuest Labs
	Intezer	Code analysis from Intezer
	ReversingLabs	File reputation & intelligence from ReversingLabs TitaniumCloud
	Spamhaus_HBL	File reputation from Spamhaus Hash Blocklist (HBL)
	Triage	Dynamic malware analysis from Hatching Triage
	UnpacMe	Malware unpacking service from UnpacMe
	VMRay	Dynamic malware analysis from VMRay
	YOROI_YOMI	Dynamic malware analysis from YOROI YOMI
comments	id	Unique id that identifies this comment
	date_added	Timestamp (UTC) when this comment has been made
	twitter_handle	Twitter handle who wrote this comment
	display_name	Twitter display name
	comment	The comment itself

Di seguito sono riportati gli STIX Object utilizzati per descrivere le informazioni estratte dal connettore:

5.3.1 Report

PROPERTY	REQUIRED	TYPE
report_types		REPORT_TYPE
description		String
name	YES	String
labels		List(String)
created_by_ref		Reference(Identity)
published	YES	TimeStamp
object_refs	YES	List(Reference(SDO))
external_references		List(ExternalReference)

5.3.2 Relationship

PROPERTY	REQUIRED	TYPE
relationship_type	YES	String
source_ref		Reference(SOURCE_REF)
target_ref		Reference(TARGET_REF)
confidence		Integer

5.3.3 Identity

PROPERTY	REQUIRED	TYPE
name	YES	String

5.3.4 Indicator

PROPERTY	REQUIRED	TYPE
pattern	YES	PatternProperty
patter_type	YES	String
created_by_ref		String
name		String
indicator_types		List(String)
labels		List(String)

5.3.5 Note

PROPERTY	REQUIRED	TYPE
content	YES	String
object_refs	YES	List(Reference(SDO))
labels		String
external_references		List(ExternalReference)
abstract		String

5.3.6 ExternalReference

PROPERTY	REQUIRED	TYPE
url		String
description		String
source_name	YES	String

5.3.7 Malware

PROPERTY	REQUIRED	TYPE
is_familiy	YES	Boolean
name		String
description		String
labels		String
first_seen		DateTime
last_seen		DateTime
external_references		List(ExternalReference)

5.4 Creazione bundle (stix2)

I bundle sono stati creati con Identity, Malware, Report, Note, Indicator, Relationship e relazionati tra di loro.

Identity	Malware	Relationship	Indicator	Report	Note
----------	---------	--------------	-----------	--------	------

6. Casi d'uso

6.1 Ricerca IOC riguardo la vulnerabilità 'log4shell' di log4j

Log4Shell è una vulnerabilità presente nella libreria Log4j. Apache Logging Project (Apache Log4j) è un framework di logging open source scritto in Java e distribuito da Apache Software Foundation che gli sviluppatori utilizzano per tenere traccia dell'attività del software nelle app cloud e aziendali. Ciò significa che è utilizzato in tantissimi dispositivi (IoT, kit medici e altro ancora), lo usa anche Ingenuity, l'elicottero Linux-based che vola su Marte. Una prima stima lo vedrebbe presente su circa 3 miliardi di dispositivi: secondo alcuni è la libreria di "log" più usata nel mondo Java. Per questo alcuni hanno definito il problema la più grave falla informatica degli ultimi anni.

Come possiamo vedere dall'immagine sulla piattaforma viene effettuata una ricerca per 'log4shell'. Dai risultati possiamo vedere come la piattaforma ha avuto dei riscontri di tipo Attack Pattern, Indicator e Report generati dal connettore 'Security Affairs'.

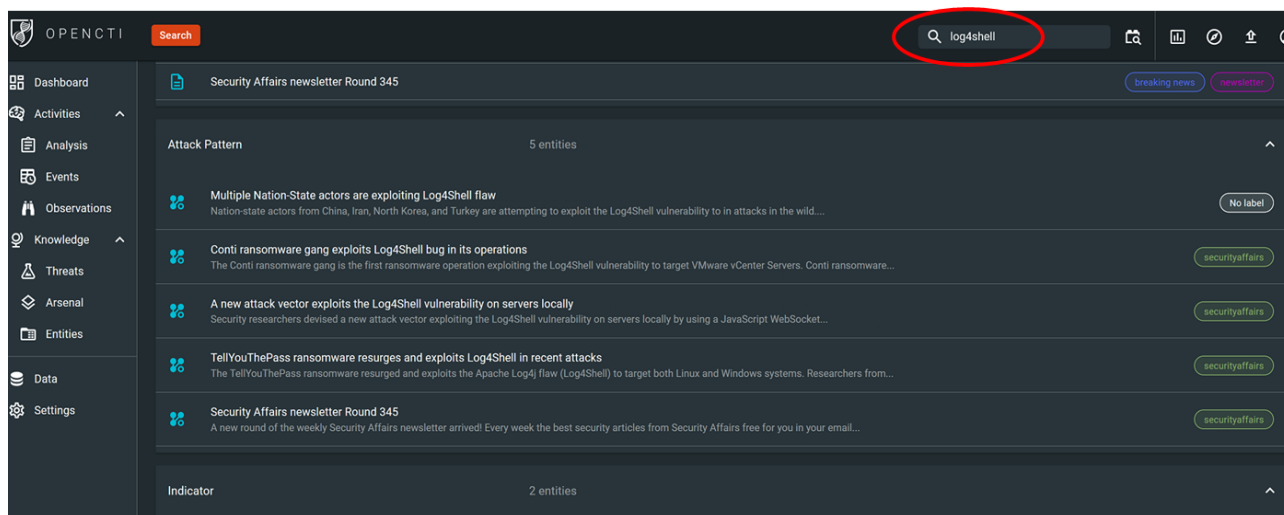


Figura 1 - Ricerca Entry relative a vulnerabilità Log4Shell.

6.2 Ricerca IOC riguardo 'CVE-2021'

Il Common Vulnerabilities and Exposures, o CVE, è un dizionario di vulnerabilità e falle di sicurezza note pubblicamente.

L'identificazione univoca delle CVE permette una maggiore comunicazione nel mondo della sicurezza e aiuta nella valutazione della diffusione di servizi e strumenti.

Si sono ricercati tutti i CVE creati nel 2021, nei risultati vediamo tutti i risultati che la piattaforma ha generato.

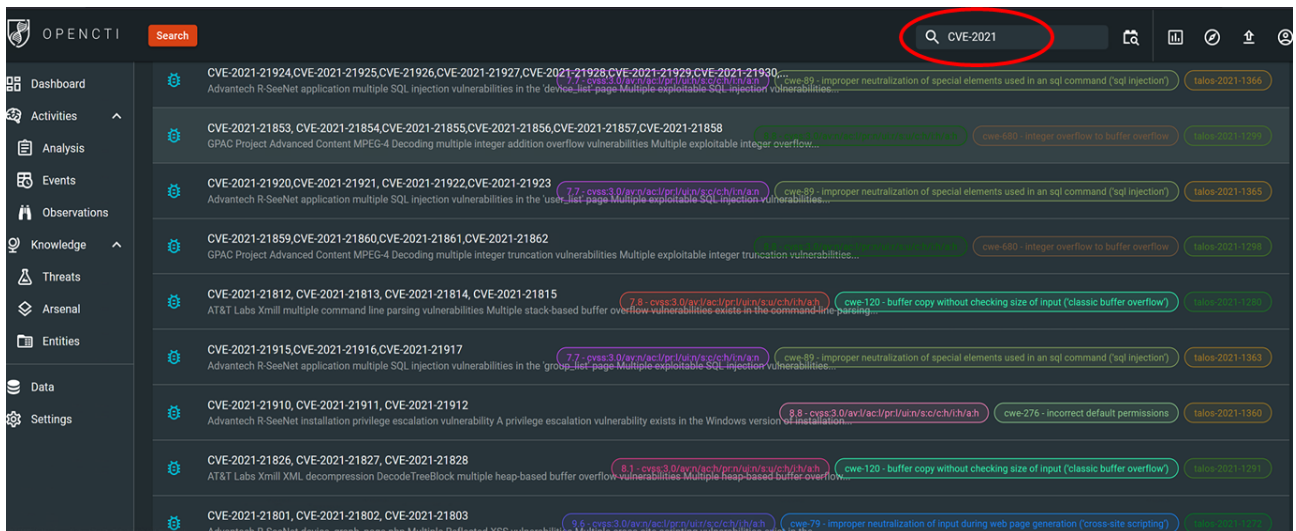


Figura 2 - Ricerca Entry relative a vulnerabilità CVE-2021

Nella figura 3 è possibile vedere nel dettaglio una delle vulnerabilità presente nei riscontri della piattaforma generata in questo caso dal connettore 'Talos Intelligence'.

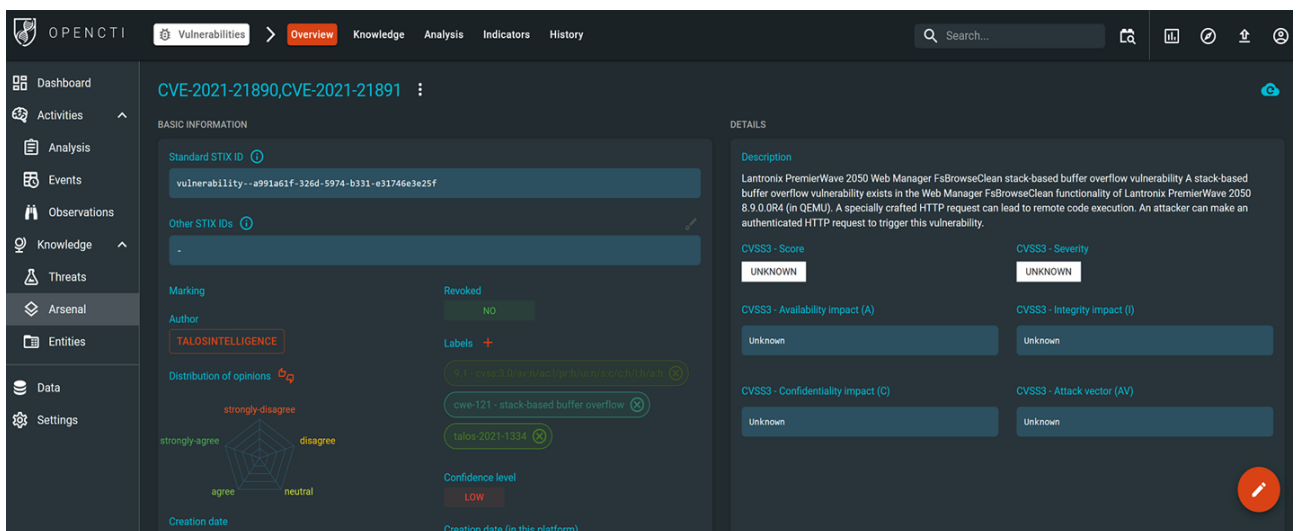
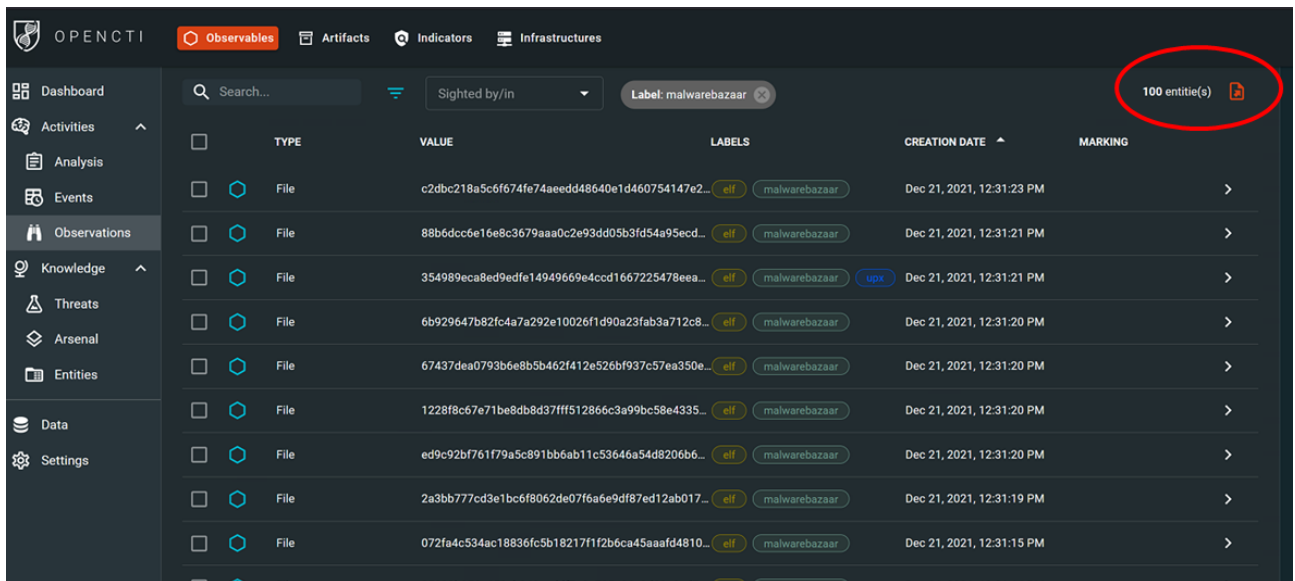


Figura 3 - Report relativo a vulnerabilità CVE-2021

6.3 Export IOC

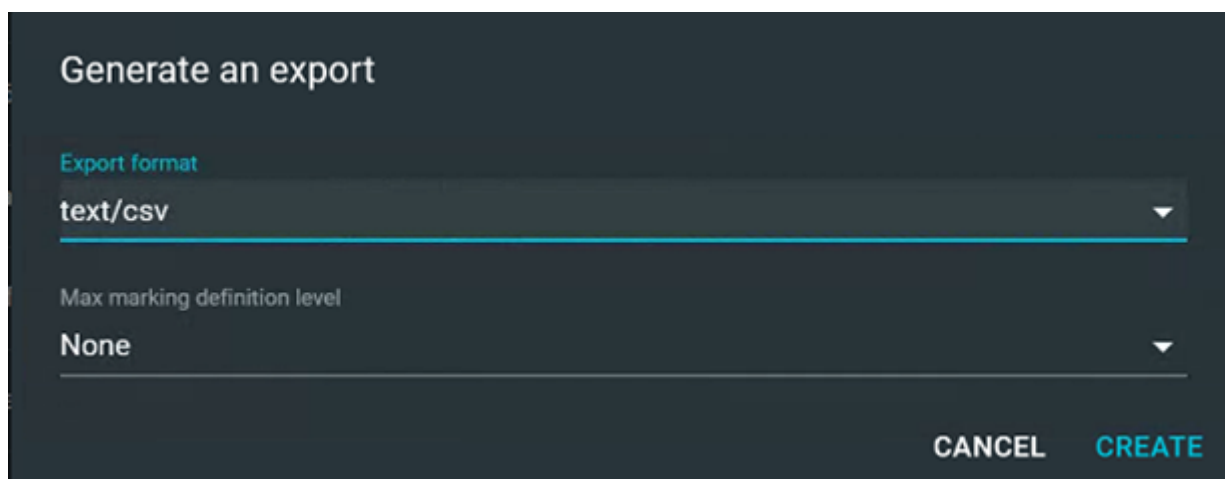
La piattaforma OpenCTI permette l'export dei dati in vari formati. Il caso d'uso corrente si focalizza sull'esportazione degli IOC relativi agli observables prodotti dal connettore MalwareBazaar. Nella figura 4 è possibile vedere nello specifico la lista degli observables da esportare e il pulsante da premere per avviare la procedura.

Una volta premuto il pulsante viene mostrata la finestra di selezione formato, da dove è possibile scegliere uno dei formati supportati dai connettori di default. nella figura 4.1 è possibile vedere la finestra di export.



	TYPE	VALUE	LABELS	CREATION DATE	MARKING
<input type="checkbox"/>	File	c2dbc218a5c6f74fe74aeedd48640e1d460754147e2...	elf malwarebazaar	Dec 21, 2021, 12:31:23 PM	>
<input type="checkbox"/>	File	88b6dcc6e16e8c3679aaa0c2e93dd05b3fd54a95ecd...	elf malwarebazaar	Dec 21, 2021, 12:31:21 PM	>
<input type="checkbox"/>	File	354989eca8ed9edfe14949669e4ccd1667225478eea...	elf malwarebazaar uox	Dec 21, 2021, 12:31:21 PM	>
<input type="checkbox"/>	File	6b929647b82fc4a7a292e10026f1d90a23fab3a712c8...	elf malwarebazaar	Dec 21, 2021, 12:31:20 PM	>
<input type="checkbox"/>	File	67437dea0793b6e8b5b462f412e526bf937c57ea350e...	elf malwarebazaar	Dec 21, 2021, 12:31:20 PM	>
<input type="checkbox"/>	File	1228f8c67e71be8db8d37fff512866c3a99bc58e4335...	elf malwarebazaar	Dec 21, 2021, 12:31:20 PM	>
<input type="checkbox"/>	File	ed9c92bf761f79a5c891bb6ab11c53646a54d8206b6...	elf malwarebazaar	Dec 21, 2021, 12:31:20 PM	>
<input type="checkbox"/>	File	2a3bb777cd3e1bc6f8062de07f6a6e9df87ed12ab017...	elf malwarebazaar	Dec 21, 2021, 12:31:19 PM	>
<input type="checkbox"/>	File	072fa4c534ac18836fc5b18217f1f2b6ca45aaafd4810...	elf malwarebazaar	Dec 21, 2021, 12:31:15 PM	>

Figura 4 - Lista Observables



Generate an export

Export format

text/csv

Max marking definition level

None

CANCEL CREATE

Figura 4.1 - Finestra Export

Una volta scelti dati da esportare e formato dati, che può variare con i connettori di default fra:

- text/csv
- text/plain
- pdf
- StixFile

il file può essere scaricato e aperto con un comune software come Excel per la visualizzazione dei dati esportati, come viene riportato in figura 4.2.

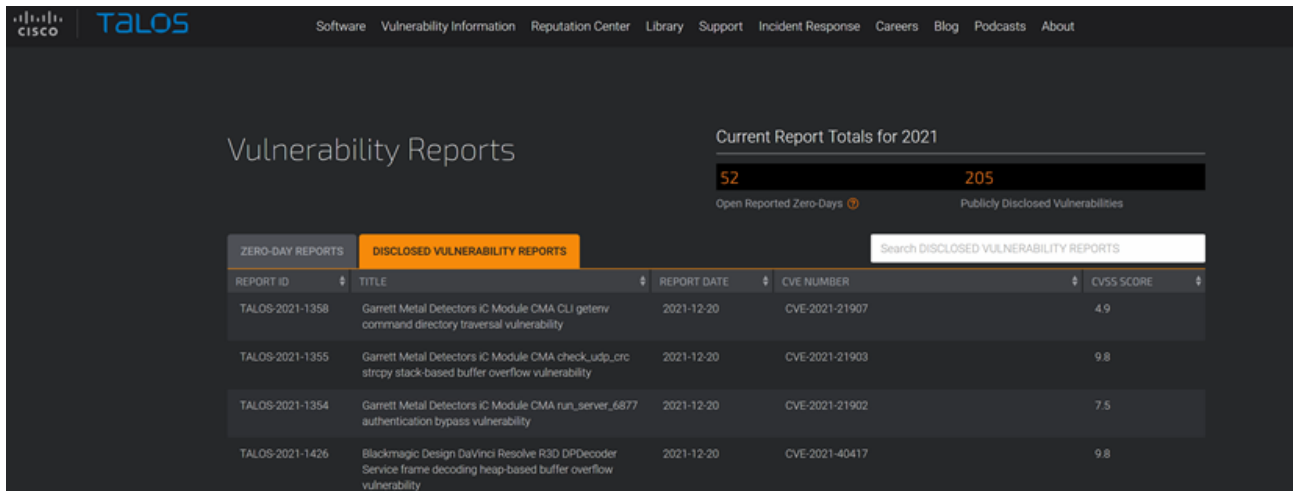
created	createdBy	createdBy	created_a description	entity_type	externalR	externalR id	importFile	importFile	modified
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Multiple flaws in the Log4j library are scaring	Report		0aa1fb9c-7c1bac35-016d-41a8-8e4f-b3ca	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: A cyber attack hit four affiliated online sports gear	Report		0046b407-9db0082-0e64-4514-b0d0-0c9	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: The Conti ransomware gang is the first ransomware	Report		0046b407-b93820b2-edf7-4c3e-aa48-6b34	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: VMware released security patches for a critical	Report		0046b407-12e1bfe7-a486-43d0-a021-7820	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Experts reported the resurgence of the Phorpiex	Report		40948476-3fd17f3f-389f-4aa1-8d2d-49d7c	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Tens of thousands of devices worldwide, including	Report		92422b4e-9dd0dc42-271e-4d75-9e64-0e4	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: The ImControllerService service of Lenovo	Report		0aa1fb9c-007bf6e8-6694-47b4-a840-575e	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Experts warn that threat actors are actively	Report		0aa1fb9c-b2ba5022-19c9-4687-a24b-aaaa	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Nation-state actors from China, Iran, North Korea,	Report		904b112b-7d5aa92b-8cae-4584-9c8c-03db	2021-12-1		2021-12-1
2021-12-1	SecurityA	03af2dbf-	2021-12-1: Threat actors are using a malicious Internet	Report					2021-12-1

name	objectLab	objectLab	objectMar	objectMar	objects	objectsids	parent_ty	published	report_ty	revoked	spec_vers	standard	_updated_at
Apache releases the	3e394553-248a-47b3-9744-d374	Apache re	8732cb7f-	Basic-Obj	2021-12-1	note					2.1	report--cc	2021-12-18T15:44:56.500Z
1.8 Million customer	c7c01669-b2dc-4f30-8175-c6bd	1.8 Millior	b808bef1-	Basic-Obj	2021-12-1	note					2.1	report--d	2021-12-18T15:44:51.835Z
Conti ransomware g	bfb8a02e-ff2a-4f83-a702-e3d0	Conti rans	57db0193-	Basic-Obj	2021-12-1	note					2.1	report--4e	2021-12-18T15:45:02.275Z
VMware fixes critica	7d825ae1-a3b8-4ea4-87d7-540	VMware f	d1e453de	Basic-Obj	2021-12-1	note					2.1	report--a1	2021-12-18T15:45:08.366Z
Phorpiex botnet is b	1e1a458d-9fc7-4891-96e6-54d1	Phorpiex	149d5c071-	Basic-Obj	2021-12-1	note					2.1	report--d	2021-12-18T15:45:13.223Z
PseudoManuscript,	dbb18855-7a48-4126-a31a-15fd	PseudoMi	c7641bb8-	Basic-Obj	2021-12-1	note					2.1	report--f6	2021-12-18T15:44:59.415Z
Flaws in Lenovo lapt	42f8135f-e67b-4b99-90d9-00fe	Flaws in L	e002ec2a-	Basic-Obj	2021-12-1	note					2.1	report--cc	2021-12-18T15:45:12.807Z
While attackers begi	e43b5d76-9a68-4ba9-96ab-cd9	While att	3a267b6f-	Basic-Obj	2021-12-1	note					2.1	report--fa	2021-12-18T15:45:10.735Z
Multiple Nation-Stat	720f7e14-31dd-4e73-bd0c-f7a6	Multiple	f d1841a1f-	Basic-Obj	2021-12-1	note					2.1	report--1e	2021-12-18T15:45:05.785Z
Owowa, a malicious	8e1e0292-e2c7-4d76-9f6a-7a2c	Owowa, a	8330ca4e-	Basic-Obj	2021-12-1	note					2.1	report--0f	2021-12-18T15:45:10.796Z

Figura 4.2 - File esportato in formato CSV

6.4 Ricerca IOC riguardo 'CVE-2021-1384'

Per questo caso d'uso è stato estratto un CVE da un entry della tabella delle vulnerabilità disclosed sul sito di Talos Intelligence.



REPORT ID	TITLE	REPORT DATE	CVE NUMBER	CVSS SCORE
TALOS-2021-1358	Garrett Metal Detectors IC Module CMA CLI getenv command directory traversal vulnerability	2021-12-20	CVE-2021-21907	4.9
TALOS-2021-1355	Garrett Metal Detectors IC Module CMA check_udp_crc strcpy stack-based buffer overflow vulnerability	2021-12-20	CVE-2021-21903	9.8
TALOS-2021-1354	Garrett Metal Detectors IC Module CMA run_server_6877 authentication bypass vulnerability	2021-12-20	CVE-2021-21902	7.5
TALOS-2021-1426	Blackmagic Design DaVinci Resolve R3D DPDecoder Service frame decoding heap-based buffer overflow vulnerability	2021-12-20	CVE-2021-40417	9.8

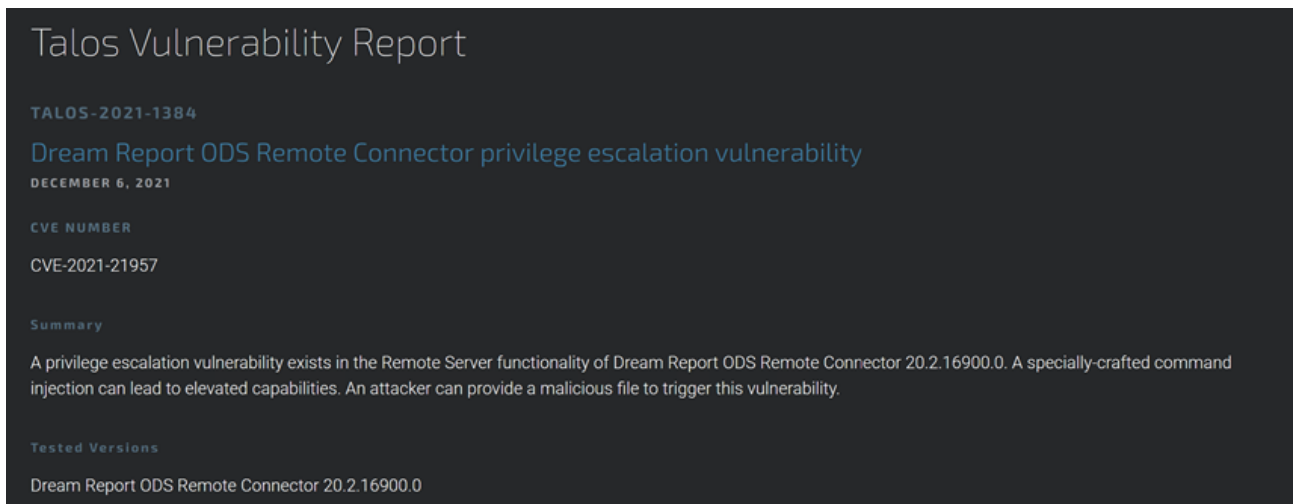
Figura 5 - Tabella delle Discloseds Vulnerability di Talos .

Nella figura 6 è possibile vedere nello specifico la vulnerabilità scelta.

TALOS-2021-1384	Dream Report ODS Remote Connector privilege escalation vulnerability	2021-12-06	CVE-2021-21957	8.8
-----------------	--	------------	----------------	-----

Figura 6 - Vulnerabilità selezionata dalla Tabella.

Nella figura 7 è possibile vedere la descrizione della vulnerabilità presente sul sito Talos Intelligence.



TALOS-2021-1384
Dream Report ODS Remote Connector privilege escalation vulnerability
DECEMBER 6, 2021
CVE NUMBER
CVE-2021-21957
Summary
A privilege escalation vulnerability exists in the Remote Server functionality of Dream Report ODS Remote Connector 20.2.16900.0. A specially-crafted command injection can lead to elevated capabilities. An attacker can provide a malicious file to trigger this vulnerability.
Tested Versions
Dream Report ODS Remote Connector 20.2.16900.0

Figura 7 - Dettaglio della vulnerabilità su Talos Intelligence.

Nella figura 8 è possibile vedere la ricerca della vulnerabilità 'CVE-2021-21952' sulla piattaforma OpenCTI, essa ha avuto vari riscontri come: Vulnerability, Indicator, Report, Attack Pattern, URL, Ipv4.

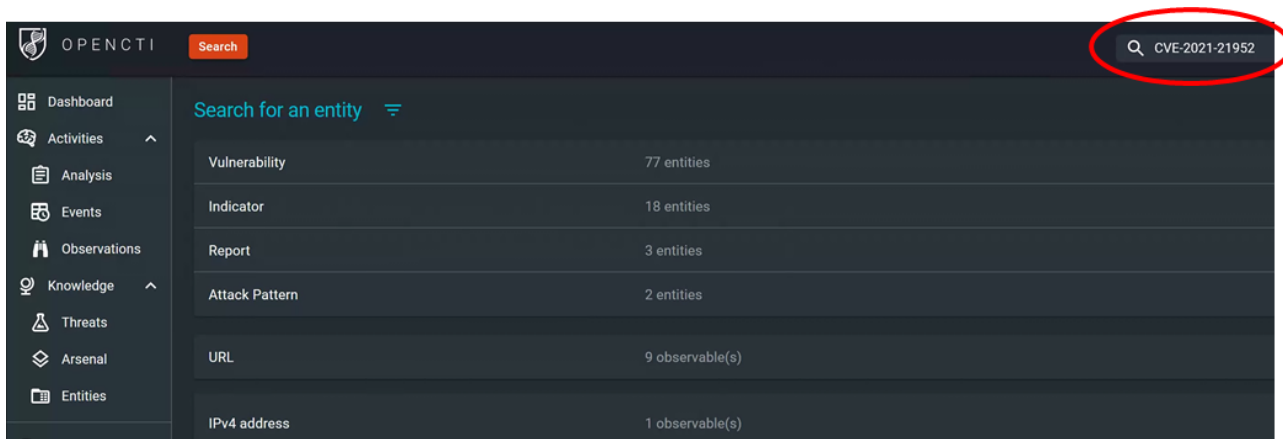


Figura 8 - Ricerca Entry relative a vulnerabilità CVE-2021-21952.

Nella figura 9 è possibile vedere nel dettaglio un Attack Pattern relativo alla vulnerabilità ricercata, tale report è stato generato dal connettore Security Affairs.

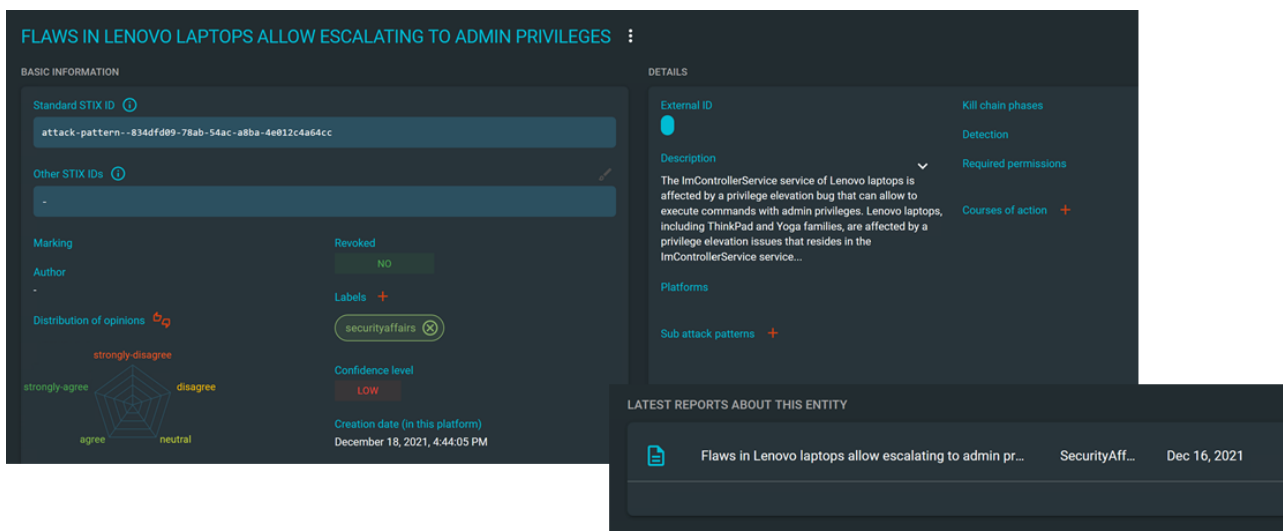


Figura 9 - Report relativo ad Attack pattern.

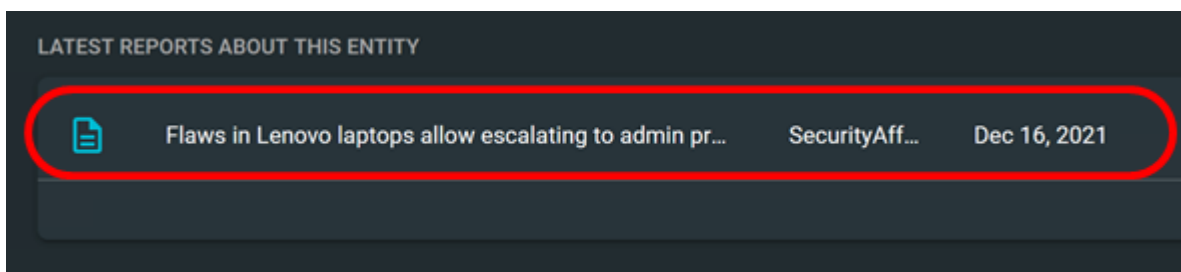


Figura 10 - Zoom-In dell'entry.

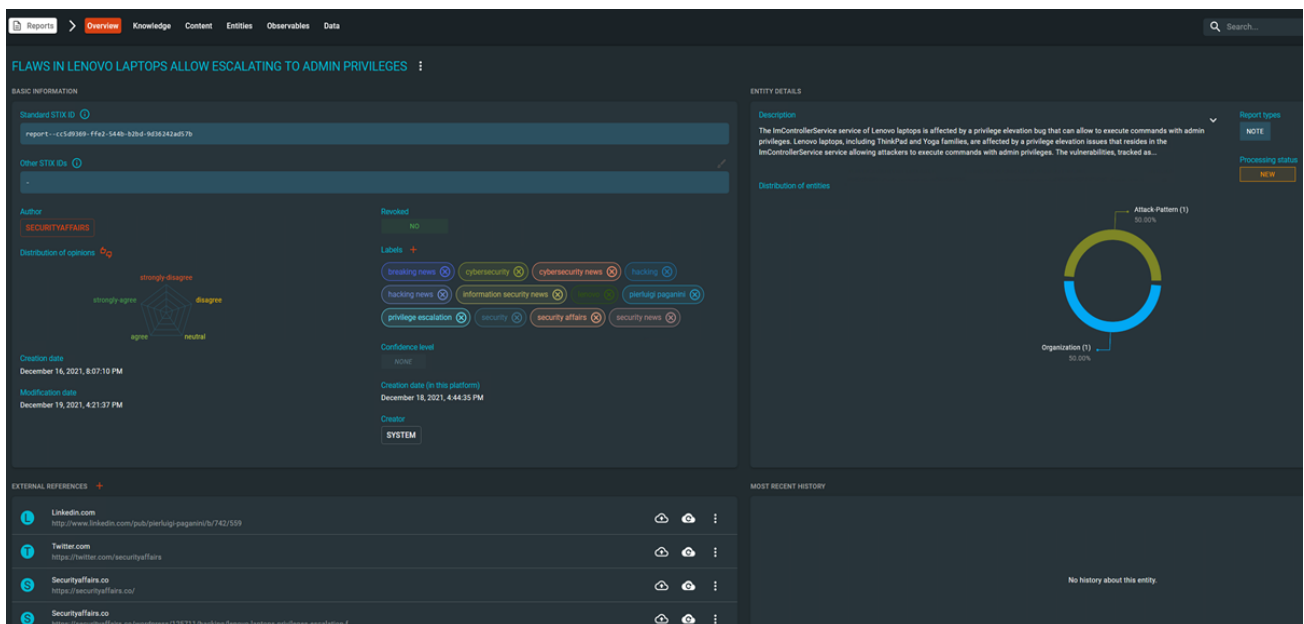


Figura 11 - View completa dell'attack pattern.

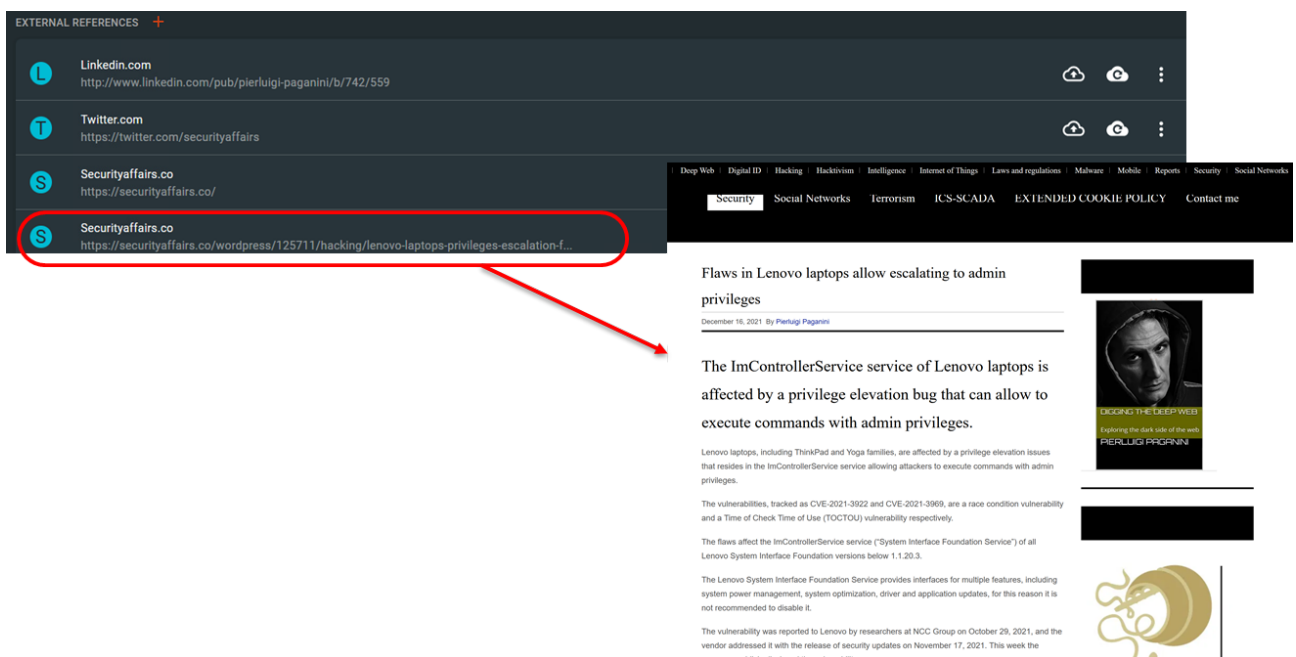


Figura 12 - Dettaglio dell'external reference dell'Attack Pattern e Articolo relativo su Security Affairs.

Nella figura 12 è possibile vedere le external reference associate all'attack pattern generato dal connettore Security Affairs correlato alla vulnerabilità ricercata. Nello specifico è stato selezionato il referral link associato alla pagina dell'articolo presente sul blog Security Affairs.