Università degli Studi di Bari “Aldo Moro”

Dipartimento di Informatica

Corso di laurea in   
**Informatica e Tecnologie per la Produzione del Software**

Tesi di laurea in

**Cybersecurity**

**Definizione di Metodi e Tecniche per la Gestione del Rischio**  
Relatori:

**Chiar.mo Prof. Danilo CAIVANO**

**Dott.ssa Vita Santa BARLETTA**

Laureando:

**Nicola BALZANO**

Anno Accademico 2023/2024

**Indice**

[Capitolo I 6](#_Toc163994636)

[Introduzione 6](#_Toc163994637)

[Capitolo II 8](#_Toc163994638)

[Cybersecurity Knowledge Base 8](#_Toc163994639)

[2.1 Internet of Things – Un mondo interconnesso 8](#_Toc163994642)

[2.2 Cybersecurity – Cos’è e di cosa si occupa 9](#_Toc163994643)

[2.3 Cyber Kill Chain – Cos’è e come usarla 9](#_Toc163994644)

[2.4 APT e Indicatori 12](#_Toc163994645)

[2.5 CPE – CVE – CWE – CAPEC – ATT&CK 13](#_Toc163994646)

[2.6 MITRE ATT&CK Framework 15](#_Toc163994647)

[2.7 MITRE ATLAS – Nuove tecnologie e nuove minacce 18](#_Toc163994648)

[2.8 Mappatura CVE – ATT&CK 19](#_Toc163994649)

[2.8.1 Mappings – Explorer 19](#_Toc163994650)

[2.8.2 Sentence Similarity Model 20](#_Toc163994651)

[Lo Stato dell’Arte 23](#_Toc163994652)

[2.9 Analisi di un reale attacco con MITRE ATT&CK 23](#_Toc163994653)

[2.9.1 Reconaissance 24](#_Toc163994654)

[2.9.2 Initial Acces 24](#_Toc163994655)

[2.9.3 Exploitation 25](#_Toc163994656)

[2.9.4 Lateral movement 25](#_Toc163994657)

[2.9.5 Discovery 26](#_Toc163994658)

[2.9.6 Defense evasion & Privilege Escalation 26](#_Toc163994659)

[2.9.7 Execution 27](#_Toc163994660)

[2.9.8 Impact 27](#_Toc163994661)

[2.10 Attacchi Cyber – Analisi delle tendenze 29](#_Toc163994662)

[2.10.1 Q2 2022 vs Q3 2023 29](#_Toc163994663)

[2.10.2 Provenienza delle cyber minacce 30](#_Toc163994664)

[2.10.3 Stime dei costi futuri 30](#_Toc163994665)

[2.11 NIS2 – L’ultima normativa nel mondo cyber 31](#_Toc163994666)

[Capitolo III 33](#_Toc163994668)

[Sperimentazione 33](#_Toc163994669)

[3.1 Dominio 33](#_Toc163994670)

[3.1.1 Framework, librerie e modelli utilizzati per il dominio 33](#_Toc163994671)

[3.1.2 Tipo di dati manipolato – STIX Object e dizionari 34](#_Toc163994672)

[Strutturazione package e directory 36](#_Toc163994673)

[3.1.3 Singleton 36](#_Toc163994674)

[3.1.4 Interfaccia per MITRE data 36](#_Toc163994675)

[3.1.4.1 mitreData 37](#_Toc163994676)

[3.1.4.2 Conversion Type 41](#_Toc163994677)

[3.1.5 Business 42](#_Toc163994678)

[3.1.5.1 MySTIXObject 43](#_Toc163994679)

[3.1.5.2 Attack Phase 43](#_Toc163994680)

[3.1.6 Container 45](#_Toc163994681)

[3.1.6.1 My STIX Container 45](#_Toc163994682)

[3.1.6.2 Attack to CVE Container 46](#_Toc163994683)

[Bibliografia 48](#_Toc163994684)

testing guide di owasp

guida per penetration test

**fortify**

**nessus**

# Capitolo I

Introduzione

Nell'era digitale in cui viviamo, **l'informatica** e la **cybersecurity** sono diventate componenti fondamentali della nostra **esistenza** **quotidiana**. Questo legame inscindibile tra tecnologia e sicurezza informatica è al centro della presente tesi, che esplora non solo come l'informatica ha plasmato il mondo moderno, ma soprattutto come la cybersecurity è diventata una materia indispensabile per proteggere i dati e le infrastrutture che sostengono la nostra società. Il mondo sta andando incontro all’evoluzione, giorno dopo giorno, mese dopo mese, anno dopo anno. L’**evoluzione** però non è solo positiva: ogni scoperta può essere interpretata sia come un progresso benefico, sia come una possibilità di impiego dannoso.

Nell'ambito della sicurezza informatica, la distinzione tra uso **legittimo** e **malintenzionato** delle nuove tecnologie è delineata da una linea estremamente sottile. Per anticipare, identificare e difendere efficacemente le infrastrutture digitali dalle minacce emergenti, diventa cruciale adottare un approccio proattivo, che sia costantemente aggiornato. In questo contesto, ciò che distingue l'uso legittimo da quello malevolo non è tanto la **conoscenza** in sé, quanto piuttosto gli **intenti** che guidano il suo impiego. Le tecniche di attacco evolvono di pari passo con le tecnologie di difesa, generando un **ciclo** **continuo** di sfide e risposte. Questa dinamica impone agli esperti di sicurezza informatica di andare oltre la semplice reazione agli incidenti, spingendoli a prevedere e prevenire attivamente le potenziali minacce.

Adottare tale approccio multidisciplinare, che integra una profonda comprensione delle **tattiche**, **tecniche** e **procedure** (**TTP**) impiegate dagli aggressori con l'uso di strumenti all'avanguardia come l'**analisi** **comportamentale**, la **threat** **intelligence** e l'**apprendimento** **automatico**, consente di anticipare e neutralizzare le minacce informatiche prima che queste si trasformino in attacchi concreti e dannosi. La capacità di rilevare precocemente le anomalie e i potenziali pericoli, analizzando e interpretando i segnali deboli all'interno del vasto mare di dati generati dalle attività di rete, rappresenta un pilastro fondamentale nella costruzione di un ecosistema digitale resiliente e sicuro.

In questo contesto, l'obiettivo primario della presente tesi è esattamente quello di esplorare e delineare l'importanza di un approccio proattivo nella sicurezza informatica, attraverso l'analisi dettagliata delle strategie offensive e difensive, insieme all'**implementazione** **di soluzioni innovative per la prevenzione e il rilevamento** di ogni possibile minaccia conosciuta.

# Capitolo II

Cybersecurity Knowledge Base

Per acquisire una piena comprensione del panorama della cybersecurity e metodi per per la gestione del rischio, bisogna conoscere l’ambiente in cui ormai l’uomo da anni si muove e le tecnologie attualmente utilizzabili.



## Internet of Things – Un mondo interconnesso

Il concetto dell’**Internet delle Cose** [1] (**IoT**[[1]](#footnote-2)) è alla base della vita smart[[2]](#footnote-3) che l’uomo vive ogni giorno, descrive dispositivi dotati di sensori, capacità di elaborazione, software e altre tecnologie che collegano e scambiano dati con altri dispositivi e sistemi su Internet o altre reti di comunicazione.

La riflessione su chi detenga la vera conoscenza, se **siamo noi a esplorare il mondo o** se **è il mondo a scrutarci dettagliatamente**, assume un rilievo particolare nell'era attuale, dominata dalla presenza capillare di dispositivi connessi. Questi strumenti, progettati per agevolare la nostra esistenza, entrano nella sfera della nostra **privacy** per nostra stessa scelta, sollevando interrogativi imprescindibili: quali dati raccolgono su di noi? Con quale precisione possono anticipare i nostri interessi e desideri di acquisto? E come fanno a mappare così accuratamente le nostre routine quotidiane? Ancor più cruciale è comprendere le potenziali implicazioni legate alla divulgazione di queste informazioni personali.

Il compito della materia d’argomento di questo elaborato è proprio quello di rispondere all’ultima domanda.

## Cybersecurity – Cos’è e di cosa si occupa

La **Cybersecurity** [2]è una materia che ha il compito di **proteggere**, nel senso più ampio del termine, **infrastrutture** **digitali** come sistemi, reti e programmi software da attacchi informatici, finalizzati all’ottenimento, trasformazione, distruzione, di informazioni sensibili e/o interruzione di processi aziendali.

Al cuore della cybersecurity vi è la triade **CIA** [3] (Confidentiality, Integrity, Availability) che funge da pilastro per la sicurezza delle informazioni. Questo modello si prefigge di garantire la **riservatezza** (**Confidentiality**) proteggendo le informazioni sensibili dall'accesso non autorizzato, l'**integrità** (**Integrity**) assicurando che i dati non vengano alterati o distrutti in modo improprio, e la **disponibilità** (**Availability**) mantenendo l'accesso continuo e ininterrotto alle informazioni e ai sistemi per gli utenti autorizzati.

Insieme, questi principi formano il framework su cui si basano le strategie di difesa contro gli attacchi informatici, che puntano a violare queste fondamenta per infliggere danni o trarre vantaggi illeciti.

## Cyber Kill Chain – Cos’è e come usarla

Per poter prevenire che accada qualsiasi tipo di incidente in natura di sicurezza informatica, bisogna comprendere a pieno come questi vengono messi in atto. Il modello che descrive le fasi con cui avviene un cyber-attacco è stato concretizzato e definito come **Cyber Kill Chain** [8] (figura 1).

È fondamentale analizzare e capire in dettaglio la Cyber Kill Chain per implementare efficacemente misure di prevenzione e difesa. Questo modello, sviluppato per descrivere le fasi sequenziali di un attacco informatico, offre agli esperti di sicurezza una visione strutturata dei processi attraverso cui un aggressore pianifica e esegue un attacco.



Figura 1: Fasi della Cyber Kill Chain

Le *fasi* di cui è composta la Cyber Kill Chain sono:

1. **Reconaissance**: volta a ottenere informazioni sulla vittima al fine di capire le modalità con cui agire successivamente. Può essere svolta in due modalità:
   1. ***Passiva***: utilizza metodi che non permettono all’individuo/organizzazione target di essere individuati (es. Domain Names, whois, Social Network).
   2. ***Attiva***: permette di ottenere un profilo del target più specifico ma potrebbe mettere in allerta la vittima (es. Port scanning and Services).
2. **Weponaize**: ha lo scopo di progettare il metodo con cui agire, tramite le informazioni ottenute precedentemente, progettando e sviluppando due componenti:
   1. ***RAT***: *Remote Acces Tool*, è la parte di software che permette di ottenere l’accesso al sistema target quando viene eseguita sul sistema target, solitamente anche chiamata *payload of cyber-weapon*.
   2. ***Exploit***: è lo script che permette di eseguire il RAT utilizzando vulnerabilità dei sistemi/software target, tramite l’utilizzo di *CVE*.
3. **Delivery**: la parte critica della catena per un attacker[[3]](#footnote-4), l’*alto rischio* è dovuto alle possibili tracce che vengono lasciate dal cyber criminale. Nessun metodo permette di ottenere il 100% di successo in questa fase, ma anche un tentativo andato male permette di ottenere rilevanti informazioni sul target.
4. **Exploitation**: è la fase in cui vengono sfruttate le CVE per eseguire lo script sviluppato precedentemente, molte volte non è sufficiente un solo *exploit*, bensì si utilizzano *exploit kit[[4]](#footnote-5)*.
5. **Installation**: prevede l’istallazione del RAT eludendo tutti i sistemi di sicurezza della vittima (ad es. Anti-Virus, Anti-Debugger, Anti-Emulation), tramite l’utilizzo di *Rootkit* e *Bootkit*, rendendo l’accesso ai sistemi della vittima persistente.
6. **Command & Controll (C2)**: in questa fase l’attacker riesce a comunicare con i sistemi infetti, negli anni sono nate differenti strutture per portare a termine questo step:
   1. ***Struttura Centralizzata***: classica *struttura client-server*, la limitazione consiste nel numero di risorse hardware/software disponibili nel *C2 Server*.
   2. ***Struttura Decentralizzata*:** prevede l’utilizzo della modalità di *comunicazione peer-to-peer*, la quale permette alta scalabilità e tolleranza verso gli errori di trasmissione.
   3. ***Struttura basata sui Social Network***: permette di passare le informazioni tramite l’utilizzo di social network (es. *Taidoor*)
7. **Act on Objective**: l'ultima fase della Cyber Kill Chain, implica *il raggiungimento dell'obiettivo* *prefissato* dall'aggressore. Dopo aver stabilito una presenza solida all'interno del sistema e aver ottenuto il controllo necessario tramite le fasi precedenti, l'attaccante esegue le azioni finali che possono variare a seconda delle sue intenzioni. Queste possono includere il furto di dati sensibili, la distruzione di informazioni critiche o asset aziendali o qualsiasi altro obiettivo malevolo (ad es. Ransoware, BOTNets, DDos, ZeroDay, Data exfiltration).

## APT e Indicatori

Per via dell’avanzamento delle tecnologie difensive del **blue team[[5]](#footnote-6)**, anche il **red team[[6]](#footnote-7)** si è evoluto dando via ad una nuova classe di minacce, denominate **APT** (**Adavanced Persistent Threat**) [9].

Questi nuovi metodi di attacco sono volti all’**utilizzo di tools avanzati** e tecniche progettate per **eludere** **le** **convenzionali** **difese**.

L’unico modo per difendersi da questo tipo di minacce è utilizzare metodi di ***Intellience-driven Computer Network Defense***, cioè un processo continuo basato su una strategia di gestione del rischio che mira a rilevare le minacce, includere le analisi sugli avversari, le loro capacità, obbiettivi e limitazioni.

Per utilizzare questo metodo di rilevazione delle APT, vengono impiegati specifici **identificatori** o **indicatori di compromissione** (**IoC**) [9] i quali possono essere suddivisi in tre categorie:

* **Atomici**: non posso essere suddivisi in parti più piccole (come l’indirizzo IP)
* **Calcolati**: derivano da dati coinvolti in un incidente (come i valori hash)
* **Comportamentali**: maggiormente utilizzati, sono collezione di indicatori atomici e calcolati in combinazione logica tra loro.

## CPE – CVE – CWE – CAPEC – ATT&CK

Le **Common Platform Enumeration** (**CPE**) sono uno standard per denominare e catalogare versioni specifiche di sistemi operativi, applicazioni software e dispositivi hardware. Mantenute dalla MITRE Corporation, le CPE mirano a fornire un modo univoco e standardizzato per identificare e descrivere i prodotti in modo che sia possibile correlarli facilmente con le informazioni sulle **CVE**.

Le **Common Vulnerabilities and Exposures** (**CVE**) [14], sono un catalogo pubblico di identificatori di vulnerabilità e falle di sicurezza, mantenuto dalla **MITRE Coporation**, ormai da anni queste sono uno dei principali metodi di identificazione univoco delle minacce.

La caratteristica distintiva delle CVE è l'assegnazione di un identificativo unico, o ID CVE, ad ogni vulnerabilità registrata. Originariamente, dal loro inizio nel 1999, gli ID CVE seguivano il formato CVE-YYYY-NNNN, dove "YYYY" rappresentava l'anno di identificazione della vulnerabilità e "NNNN" era un numero sequenziale che poteva arrivare fino a 9999 per ciascun anno, limitando il numero totale di vulnerabilità che potevano essere univocamente identificate in un singolo anno.

Tuttavia, a seguito dell'incremento esponenziale nel numero di vulnerabilità scoperte annualmente, dal 13 Gennaio 2015 è stato adottato un nuovo formato per gli identificatori CVE. Questo nuovo schema mantiene la parte dell'anno (CVE-anno-) ma sostituisce il numero sequenziale con una sequenza di cifre di lunghezza arbitraria, garantendo che l'ultimo campo abbia almeno quattro caratteri. Questa modifica non solo permette una capacità illimitata nell'assegnazione degli ID, ma assicura anche la retrocompatibilità con il formato precedente.

Parallelamente al sistema delle CVE, le **Common Weakness Enumeration** (**CWE**) [15] rappresentano un altro strumento fondamentale nel campo della sicurezza informatica, focalizzandosi sulle debolezze e difetti nel design e nell'implementazione del software che possono portare a vulnerabilità. Mentre le CVE forniscono un catalogo di vulnerabilità specifiche e note, le CWE offrono una vista più astratta, categorizzando tipologie di debolezze che sono comunemente sfruttate dagli aggressori.

La sinergia tra CVE e CWE si rivela estremamente utile per gli sviluppatori, i professionisti della sicurezza e le organizzazioni che mirano a migliorare le pratiche di sviluppo del software e a fortificare le loro difese contro attacchi informatici. Le CWE, mantenute anch'esse dalla MITRE Corporation, offrono una struttura per comprendere le cause radice delle vulnerabilità, facilitando la prevenzione e la mitigazione delle stesse fin dalle fasi iniziali dello sviluppo del software.

Le CWE, attraverso la loro classificazione, permettono di **identificare** **modelli** **ricorrenti** **di** **errori** di programmazione **e** **difetti** **di** **design**, promuovendo un approccio proattivo alla sicurezza che va oltre la semplice reazione alle minacce identificate tramite CVE. Questo approccio aiuta a costruire software intrinsecamente più sicuri, riducendo la superficie di attacco disponibile agli aggressori.

Dalle CWE inoltre è possibile ricollegarsi alle **Common Attack Pattern Enumeration and Classification** (**CAPEC**), nate nel 2007, sono un dizionario di pattern di attacco conosciuti e utilizzati dagli esperti del settore per prevenire aggressioni a sistemi informatici identificate e mappate tramite il **MITRE ATT&CK Framework** (figura 2).

  
Figura 2: Tassonomia di come MITRE sfrutta CVE e CWE per creare il framework ATT&CK [16]

## MITRE ATT&CK Framework

In questo scenario in continua evoluzione, il MITRE ATT&CK Framework [10] emerge come uno strumento cruciale per la comprensione e la difesa contro le APT e altre minacce avanzate. **ATT&CK**, acronimo di ***Adversarial Tactics, Techniques, and Common Knowledge***, è una base di conoscenza pubblicamente accessibile che cataloga e descrive in modo dettagliato:

* le *tattiche* (**tactics**) e le *tecniche* (**attack patterns**) utilizzate dagli aggressori nelle loro campagne malevole, anche dette **Tactics Techniques and Procedures** (**TTPs**)
* tecniche di *riconoscimento* (**detection**)
* metodi di *mitigazione* (**course of action**)
* gruppi di attacker conosciuti (**threat group**ad es. APT3, APT29)
* dispositivi/sistemi comunemente presenti in ambienti industriali (**asset**).

Il framework mette a disposizione 3 matrici in modo da suddividere l’ambiente in cui gli attacchi possano avvenire, cioè: ***Enterprise***, ***ICS*** (***Industrial Control Systems***) e ***Mobile***.

Le *tattiche* descritte nel framework, nonché le colonne della matrice, sono:

* **Reconnaissance**: Raccogliere informazioni che possono essere utilizzate per pianificare futuri attacchi.
* **Resource** **Development**: Creare e gestire risorse utilizzate per supportare le operazioni offensive.
* **Initial** **Access**: Guadagnare l'ingresso nel network o nel sistema della vittima.
* **Execution**: Eseguire codice malevolo sul sistema della vittima per portare avanti l'attacco.
* **Persistence**: Mantenere l'accesso a lungo termine ai sistemi compromessi attraverso vari metodi, nonostante i riavvii e i cambiamenti di credenziali.
* **Privilege** **Escalation**: Ottenere livelli di accesso superiori sul sistema o network compromesso, spesso ottenendo privilegi di amministrazione.
* **Defense** **Evasion**: Evitare il rilevamento attraverso diversi mezzi, includendo la modifica del codice malevolo e l'abuso di strumenti legittimi.
* **Credential** **Access**: Rubare credenziali come nomi utente e password per ottenere ulteriore accesso all'interno dell'ambiente della vittima.
* **Discovery**: Raccogliere informazioni sull'ambiente interno per orientare gli attacchi successivi.
* **Lateral** **Movement**: Muoversi attraverso la rete per accedere a ulteriori sistemi e informazioni.
* **Collection**: Raccogliere dati di valore dall'ambiente della vittima.
* **Command** **and** **Control** (C2): Comunicare con i sistemi compromessi per controllarli a distanza.
* **Exfiltration**: Trasferire dati da un computer o rete compromessi a un luogo controllato dall'aggressore.
* **Impair Process Control**: Tecniche che portano a manipolare, danneggiare e/o disabilitare processi di controllo fisici.
* **Inhibit Response Function**: Impedire che le funzioni di sicurezza, protezione, garanzia della qualità e intervento dell'operatore rispondano a un guasto, a un pericolo o a uno stato pericoloso non fermino le azioni malevole.
* **Impact**: Operazioni mirate a distruggere, interrompere o compromettere in modo significativo le risorse della vittima.

Nella documentazione del framework in questione sono disponibili vari tool, tra cui:

* **ATT&CK Workbench**: un’applicazione che permette di esplorare creare, annotare e condividere estensioni della conoscenza MITRE ATT&CK.
* **Python Utilities**: prevede una libreria python scaricabile, da poter utilizzare per manipolare e ottenere oggetti **STIX 2.0** (**Structured Threat Information Expression**).
* **ATT&CK Navigator**: Un tool web-based progettato specificamente per esplorare la matrice del MITRE ATT&CK, consentendo agli utenti di annotare possibili combinazioni di tecniche per orchestrare un attacco o per ricostruire il percorso seguito dal red team, è il MITRE ATT&CK Navigator. Questo strumento offre una piattaforma interattiva e facilmente navigabile che permette agli analisti di sicurezza, ai ricercatori e ai membri dei red team di visualizzare le tattiche e le tecniche descritte nel framework ATT&CK.  
  Con il MITRE ATT&CK Navigator, gli utenti possono creare "**layer**" personalizzati che evidenziano specifici insiemi di tecniche utilizzate in scenari di attacco noti o ipotetici, **facilitando l'analisi delle minacce** e la **pianificazione della difesa**. La capacità di annotare e combinare diverse tecniche aiuta a comprendere come gli attaccanti potrebbero stringere insieme varie tattiche per raggiungere i loro obiettivi, offrendo così spunti preziosi per lo sviluppo di strategie di mitigazione più efficaci. Inoltre, il Navigator consente la condivisione e la collaborazione tra i team, rendendo più semplice la disseminazione delle informazioni sulle minacce e l'aggiornamento delle conoscenze sulla sicurezza informatica (figura 3).



Figura 3: Esempio di utilizzo del MITRE ATT&CK Navigator  
studio dell’unione dei gruppi APT3, APT29, APT3+APT29

## MITRE ATLAS – Nuove tecnologie e nuove minacce

Con l'ascesa e l'espansione delle tecnologie di Intelligenza Artificiale (**AI**), si è assistito non solo a un progresso significativo in vari campi, ma anche alla nascita di nuove strategie e tecniche da parte dei red team per condurre azioni malevole sfruttando o mirando a queste tecnologie avanzate.

Con lo scopo di colmare il divario di conoscenza tra il red team e il blu team, è nato il nuovo framework **Mitre ATLAS** (***Adversarial Threat Landscape for Artificial-Intelligence Systems***) [11], complementare al precedente Mitre ATT&CK.

La maggiore differenza tra il MITRE ATT&CK Framework e ATLAS risiede principalmente nel modo in cui entrambi approcciano la categorizzazione e la rappresentazione delle tattiche utilizzate dagli aggressori nel corso di un attacco informatico. Nel secondo le tattiche utilizzate dagli attacker sono:

* **Reconnaissance**
* **Resource Development**
* **Initial Access**
* **ML Model Access**: Gli avversari cercano di ottenere certi livelli di accesso ad un modello di machine learning.
* **Execution**
* **Persistence**
* **Privilege Escalation**
* **Defense Evasion**
* **Credential Access**
* **Discovery**
* **Collection**
* **ML Attack Staging**: Il red team utilizza le conoscenze *white box*[[7]](#footnote-8) del sistema target per personalizzare l’attacco.
* **Exfiltration**
* **Impact**

## Mappatura CVE – ATT&CK

### Mappings – Explorer

Per approfondire lo studio sugli impatti che ogni vulnerabilità, identificata tramite un ID CVE, può avere su un sistema informatico, la **CTID** (Center for Threat-Informed Defense) ha continuato a sviluppare un framework della **MITRE** **ENGENUITY[[8]](#footnote-9)** che facilita la correlazione tra le CVE conosciute e le tecniche descritte nel framework ATT&CK, anche se al tempo di scrittura di questo studio il framework ATT&CK to CVE lavora soltanto sul dominio *Enterprise* della matrice ATT&CK.

Nello studio svolto da CTID ad ogni CVE vengono assegnati 4 parametri (figura 4):

* **Exploitation Technique**: una lista di metodi che possono essere usati per sfruttare la vulnerabilità;
* **Primary Impact**: una lista di tecniche che identificano il beneficio inziale raggiunto;
* **Secondary Impact**: una lista di tecniche che descrivono cosa l’avversario può fare se ottiene il beneficio dell’impatto primario;
* **Uncategorized**: una lista di tecniche correlate alla CVE in questione, il cui tipo di relazione non rientra tra le precedenti.

  
Figura 4: Esempio di come una CVE è correlata al framework ATT&CK [17]

Sebbene questo framework offra un'analisi comprensiva, la correlazione tra le CVE e le TTPs del MITRE ATT&CK che mette a disposizione è aggiornata soltanto fino al 2021, risultando quindi tre anni indietro rispetto alla data di redazione di questo studio. Al fine di ampliare il dataset di mappatura tra CVE e ATT&CK si è impiegata anche un’altra tecnica relazionale compensativa.

### Sentence Similarity Model

Un **modello di similarità** tra frasi, o "**sentence similarity model**", è una forma specifica di Large Language Model (**LLM**) utilizzato nel campo dell'elaborazione del linguaggio naturale (**NLP**) per determinare quanto due frasi siano semanticamente simili l'una all'altra. Il suo scopo è quello di trasformare descrizioni testuali complesse in rappresentazioni vettoriali (detti vettori **embedding**) che riflettano il significato semantico sottostante, facilitando così l'analisi delle strategie di attacco e migliorando la comprensione delle minacce.

I vettori **embedding** [21], sono rappresentazioni numeriche ad alta dimensionalità di frasi o parole. Questi vettori catturano il contesto e il significato semantico delle entità linguistiche, trasformando il testo in un formato che può essere facilmente processato dai modelli di machine learning. Grazie ad essi il modello può discernere le sfumature semantiche tra termini diversi e riconoscere la similarità tra concetti correlati, anche se espressi con parole differenti. I vettori risultanti dall’utilizzo di tale modello semantico permettono ai ricercatori di studiare la similarità tra 2 testi, tramite vari modi, come la **similarità coseno**.

La **similarità coseno** è una metrica utilizzata per misurare quanto due vettori embedding siano simili l'uno all'altro in termini di orientamento nello spazio vettoriale, ignorando la loro magnitudine[[9]](#footnote-10).

La formula per calcolare la similarità coseno tra due vettori A e B è

Dove:

* rappresenta il prodotto scalare dei vettori A e B
* sono le magnitudini dei vettori A e B, calcolate come e rispettivamente dove e sono gli elementi dei vettori A e B

Il risultato della similarità coseno varia tra -1 e 1, dove:

* 1 indica che i due vettori sono direzionati esattamente nella stessa direzione,
* 0 indica che i vettori sono ortogonali (angolo di 90 gradi, indicando indipendenza o nessuna similarità),
* -1 indica che i vettori sono direzionati esattamente in direzioni opposte.

Questo significa che la similarità coseno valuta l'angolo tra due vettori con valori compresi tra -1 e 1, dove un valore di similarità vicino a 1 indica una forte correlazione semantica tra le frasi o le parole rappresentate dai vettori (figura 5).

Nella ricerca corrente verrà scelto un modello specificamente sviluppato per il dominio della sicurezza informatica, per analizzare e determinare il grado di similarità tra le descrizioni delle CVE e quelle delle TTPs all'interno del framework ATT&CK, con l'obiettivo di identificare possibili correlazioni. Questo approccio consente di stabilire legami diretti tra vulnerabilità specifiche e le modalità operative degli attaccanti.



Figura 5: rappresentazione grafica della similarità coseno tra due vettori

Lo Stato dell’Arte

## Analisi di un reale attacco con MITRE ATT&CK

Il cyber attacco preso in esempio è avvenuto contro il sistema internet satellitare della compagnia americana **Viasat Inc**.

Il 24 febbraio 2022, coincidendo con l'inizio dell'invasione russa dell'Ucraina, si è verificato un attacco informatico di significativa entità che ha colpito l'accesso a Internet via satellite a banda larga. Questo attacco ha specificamente mirato a disabilitare i modem utilizzati per stabilire la comunicazione con la rete satellitare **KA-SAT**, gestita da Viasat Inc, la quale appoggia una parte dei sui servizi su quelli offerti da **Skylogic**, una società specializzata in servizi di comunicazione satellitare a banda larga per le piccole e medie imprese, conglomerati industriali e il pubblico. L'effetto immediato è stata la **perdita di connettività** per decine di migliaia di utenti in Ucraina e in diverse parti dell'Europa, evidenziando la vulnerabilità delle infrastrutture critiche di comunicazione in contesti di conflitto geopolitico [12].

L'attacco informatico contro Viasat ha avuto **ripercussioni ben oltre la semplice interruzione dei servizi** di comunicazione, toccando infrastrutture critiche e numerosi utenti in diverse nazioni europee. Una significativa **compagnia** **energetica** **tedesca** ha riscontrato la perdita della capacità di monitoraggio remoto su oltre 5.800 turbine eoliche. In **Francia**, quasi 9.000 utenti di un **provider** **di** **servizi** **Internet** via satellite hanno sperimentato un'interruzione della connessione, mentre un altro fornitore ha visto circa un terzo dei suoi 40.000 abbonati in **Europa** (includendo paesi come Germania, Francia, Ungheria, Grecia, Italia e Polonia) affrontare **problemi** **di** **accesso** **a** **Internet**. In totale, l'attacco ha impattato diverse migliaia di clienti in Ucraina e decine di migliaia di utenti della banda larga fissa in tutto il continente europeo, sottolineando l'ampio raggio d'azione e le severe conseguenze che un attacco mirato può generare su scala transnazionale.

Premettendo che questo sia solo un’ipotesi, come dice la fonte [13]:

“Without first-hand knowledge of Viasat’s systems, we cannot be certain about our hypothesis”

è stato possible creare una mappatura tra le TTPs del framework MITRE ATT&CK e l’attacco precedentemente descritto.

### Reconaissance

Tutto è iniziato nel 2021, Fortinet ha rilevato un attacco sulla VPN “*Fortigate*” riguardante la vulnerabilità CVE-2018-13379 nota dal 2019. Tramite questa il gruppo di hacker russi noti con il denominativo *Groove* ha rubato credenziali di quasi 500.000 indirizzi IP, utilizzano le seguenti TTPs:

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Reconaissance | [T1595.002] Active Scanning: Vulnerability Scanning |
| [T1593] Search Open Websites/Domains |
| [T1589.001] Gather Victim Identity Information: Credentials |
| Resource Development | [T1650] Acquire Access |
| [T1586] Compromise Accounts |

### Initial Acces

Dato che i server di controllo di Skylogic, le Gateway Earth Stations e i modem Surfbeam2 impiegati da Viasat si affidano a dispositivi VPN forniti dalla società Fortinet, è chiaro che il punto di vulnerabilità sfruttato per l'intrusione era effettivamente legato a queste VPN.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Initial Acces | [T1190] Exploit Public-Facing Application |
| [T1133] External Remote Services |

### Exploitation

Le indagini condotte in seguito all'attacco hanno rivelato che l'intrusione è stata resa possibile da una configurazione errata in una Virtual Private Network (VPN), utilizzata per accedere in remoto alla rete KA-SAT.

Nonostante Fortinet avesse precedentemente rilasciato una patch per correggere la CVE identificata, sia gli operatori di Viasat che Skylogic non avevano distribuito l'aggiornamento necessario. Di conseguenza, l'accesso non autorizzato è stato facilitato attraverso le VPN non aggiornate, consentendo agli aggressori di penetrare nelle Gateway Earth Stations di Skylogic.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Initial Access | [T1078] Valid Accounts |
| Privilege Escalation | [T1068] Exploitation for Privilege Escalation |
| Defense Evasion | [T1562.004] Impair Defenses: Disable or Modify System Firewall |

### Lateral movement

Dopo aver ottenuto l'accesso iniziale attraverso le VPN non aggiornate, l'aggressore ha eseguito una movimentazione laterale all'interno della rete di gestione fiduciaria, dirigendosi verso un segmento di rete specificamente designato per il controllo e la gestione della rete di modem. Attraverso questo accesso avanzato, o escalation di privilegi, l'aggressore è stato in grado di oltrepassare la Demilitarized Zone (DMZ) e infiltrarsi nella rete intranet satellitare a tubo curvo, che rappresenta la rete di gestione fiduciaria principale utilizzata per interfacciarsi con i modem Surfbeam2.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Discovery | [T1049] System Network Connections Discovery |
| [T1082] System Information Discovery |
| Lateral Movement | [T1021] Remote Services |
| [T1570] Lateral Tool Transfer |

### Discovery

L'attacco mirato non ha colpito uniformemente tutti i modem Viasat; infatti, solo una selezione di questi è stata presa di mira. Questa specificità d'azione può essere attribuita alla capacità degli operatori situati presso le Gateway Earth Stations di dirigere il segnale verso determinate celle geografiche tra le 82 disponibili sulla rete satellitare KA-SAT. In pratica, ciò significa che l'aggressore aveva la possibilità di determinare quali specifiche aree geografiche (e di conseguenza, i modem corrispondenti situati in quelle aree) fossero destinati a ricevere il segnale contaminato da comandi malevoli. Questo approccio selettivo ha permesso all'attaccante di concentrare l'attacco su target specifici, massimizzando l'efficacia dell'operazione dannosa e limitando al contempo la possibilità di rilevazione precoce dell'attacco stesso

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Discovery | [T1016] System Network Configuration Discovery |
| [T1082] System Information Discovery |

### Defense evasion & Privilege Escalation

Una volta che l’attacker ha ottenuto l’accesso ai modem, ha utilizzato altre tecniche di privilage escalation, utilizzando la VPN senza patch.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Defense Evasion | [T1562.004] Impair Defenses: Disable or Modify System Firewall |
| Initial Access | [T1133] External Remote Services |
| Privilege Escalation | [T1068] Exploitation for Privilege Escalation |

### Execution

L’attaccate è riuscito a fornire un aggiornamento firmware valido al dispositivo, installando un binario *ELF* (*Executable and Linkable Format*) detto “*Acidrain*”, che sovrascriveva i dati chiave nella memoria flash dei modem, rendendoli impossibilitati ad accedere alla rete, ma non permanentemente inutilizzabili.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Resource Development | [T1588.002] Obtain Capabilities: Tool |
| Execution | [T1072] Software Deployment Tools |
| Initial Access | [T1195] Supply Chain Compromise |
| Defense Evasion | [T1070.004] Indicator Removal: File Deletion |
| Persistence | [T1542.001] Pre-OS Boot: System Firmware |

### Impact

In questa fase vengono descritte le ultime tecniche utilizzate per ottener egli obbiettivi prefissati.

|  |  |
| --- | --- |
| **Tattiche** | **Tecniche** |
| Impact | [T1529] System Shutdown/Reboot |
| [T1485] Data Destruction |
| [T1495] Firmware Corruption |
| [T1561] Disk Wipe |
| [T1529] System Shutdown/Reboot |
| [T1485] Data Destruction |
| [T1495] Firmware Corruption |
| [T1561] Disk Wipe |
| [T1561.001] Disk Wipe: Disk Content Wipe |
| [T1561.002] Disk Structure Wipe |
| [T1531] Account Access Removal |
| [T1498] Network Denial of Service |
| [T1489] Service Stop |

## Attacchi Cyber – Analisi delle tendenze

Negli ultimi anni, il panorama globale ha testimoniato l'urgente richiesta di avanzamenti tecnologici nel campo della difesa informatica, volti a proteggere dati, procedure e infrastrutture critici.

### Q2 2022 vs Q3 2023

Un'**indagine comparativa** recente [4], che confronta i dati relativi agli attacchi informatici noti fino al Q2[[10]](#footnote-11) 2022 e quelli registrati nel Q2 2023 (figura 6), ha evidenziato un incremento esponenziale nella media settimanale degli attacchi informatici a livello globale, interessando diversi settori industriali. Questo trend allarmante sottolinea non solo la crescente sofisticatezza e frequenza delle minacce informatiche, ma anche l'impellente necessità per le organizzazioni di ogni ambito di rafforzare le loro misure di sicurezza per contrastare efficacemente tali pericoli.

  
Figura 6: Q2 2022 vs Q2 2023

I dati allarmanti emersi dallo studio mostrano un incremento significativo degli attacchi informatici, con particolare enfasi sui settori delle consulenze, bancario e sanitario. Tra questi, il **settore** **sanitario** emerge come particolarmente **critico**, non solo perché rappresenta il terzo settore più colpito al mondo da questa ondata di attacchi, ma anche per l'ampia quantità di introiti che genera a livello globale e per il **vasto** **volume** **di** **informazioni** **sensibili** che gestisce. Questa situazione mette in luce l'urgenza con cui il settore sanitario deve affrontare le sfide legate alla cybersecurity, sottolineando l'importanza di implementare misure di protezione avanzate per salvaguardare dati di vitale importanza.

### Provenienza delle cyber minacce

Un altro grande problema dilemma è dovuto alla provenienza di questi attacchi. Uno studio [5] in cui sono coinvolte la Cybersecurity and Infrastructure Security Agency (**CISA**), la National Security Agency (**NSA**) e il Federal Bureau of Investigation (**FBI**) (figura 7), evidenzia che circa il 45% di questi attacchi ha origine ignota, perciò la **tracciabilità** e l'**identificazione** **degli aggressori** rappresentano ancora sfide significative nel contrasto alle minacce informatiche.

  
Figura 7: Da dove provengono i cyber attacchi

### Stime dei costi futuri

Basandosi sulle valutazioni della fonte che ha fornito i dati menzionati in precedenza, il **costo annuale globale associato alla mitigazione dei crimini informatici** [6] nei prossimi 4 anni è destinato ad aumentare in maniera lineare di circa **1,5 trilioni di dollari statunitensi** all’anno (figura 8).

  
Figura 8: Stima della crescita del costo annuale per il cyber crimine

## NIS2 – L’ultima normativa nel mondo cyber

Il mondo ha iniziato a mobilitarsi per rispondere alle minacce derivanti dalla evolutiva sfera informatica, molto sono state le normative che hanno coinvolto questo dominio di conoscenza.

La direttiva più recente è la cosiddetta **NIS2** (**Network and Information Systems 2**), entrata in vigore nel 17 gennaio 2023, rappresenta un passo significativo verso il rafforzamento della resilienza e della sicurezza delle reti e dei sistemi informativi all'interno dell'**Unione Europea**, dove gli stati membri dovranno incorporare questa normativa entro il 17 ottobre 2024. Questa nuova direttiva si propone di aggiornare e ampliare l'ambito di applicazione della antesignana direttiva **NIS1**, per porre rimedio all’aumento del tasso digitalizzazione in tutti i Paesi membri, il quale ha inasprito la superfice di attacco informatico.

La normativa rende più stringenti:

* **requisiti di governance**, in modo che gli organi di gestione di una struttura economica approvino misure per la *gestione dei rischi* dell’Organizzazione e una *formazione* *periodica* su tematiche di cybersicurezza;
* **gestione dei rischi**, inserendo l’obbligo di *valutare* *i* *rischi* e attuare le necessarie *misure* *tecniche* *e* *organizzative* anche nell’ambito della supply chain e rapporti con i propri fornitori**;**
* **segnalazione** **di** **incidenti** **avvenuti**, notificandoli ai rispettivi *CSIRT[[11]](#footnote-12)* o *autorità* *nazionale* entro 24 ore dall’evento.

La NIS2 mira a **stabilire** un livello comune elevato di sicurezza delle reti e dei sistemi informativi tra gli Stati membri, promuovendo al contempo una **maggiore** **cooperazione** e condivisione delle informazioni sulle minacce informatiche all'interno dell'UE. Tra le novità più rilevanti, la direttiva prevede l'istituzione di punti di contatto nazionali per la cybersecurity, l'obbligo di notifica degli incidenti informatici e l'introduzione di **sanzioni** significative **per** **le** **violazioni**, pari ad un massimo di 10.000.000 EUR.

Implementando misure come queste, la NIS2 non solo cerca di proteggere le infrastrutture critiche europee, ma anche di creare un ambiente digitale più sicuro per cittadini, imprese e governi. L'**obiettivo** è di anticipare, prevenire e rispondere efficacemente agli attacchi informatici, assicurando così la continuità dei servizi essenziali su cui la società moderna si affida profondamente.



# Capitolo III

Sperimentazione

L'obiettivo principale dello studio di tesi è lo sviluppo di un sistema avanzato progettato per offrire un supporto essenziale ai professionisti del settore della sicurezza informatica.

Il sistema proposto mira a semplificare il processo di mitigazione degli attacchi informatici diretti verso le infrastrutture digitali: attraverso l'impiego di strumenti per il riconoscimento delle CVE in sistemi informatici, la classificazione delle CVE identificate in base alle TTPs attualmente note e le conseguenti tecniche che potrebbero essere state impiegate o che potrebbero manifestarsi in futuro.

## Dominio

Durante la **fase iniziale** dello sviluppo, è stato intrapreso il processo di definizione e strutturazione del Dominio. Questo passo fondamentale ha comportato l'identificazione delle aree chiave di interesse, l'analisi delle esigenze specifiche e la mappatura delle relazioni tra i vari elementi e funzionalità che costituiranno il sistema.

Data la presenza di diversi framework implementati in **Python**, la scelta si è orientata verso l'utilizzo di questo linguaggio, prediligendo una **metodologia** di sviluppo **orientata** **agli** **oggetti** anziché funzionale.

### Framework, librerie e modelli utilizzati per il dominio

I framework utilizzati durante lo sviluppo dell’applicazione in questione sono:

* **MITRE ATT&CK**: fornisce una libreria Python, disponibile tramite il gestore di pacchetti pip o repository github [18], la quale permette di catalogare e relazionare le entità presenti nel framework, cioè: tattiche, tecniche, campagne, gruppi, software e assets.
* **MITRE ATLAS**: essendo una tecnologia ancora in fase di evoluzione e introdotta solamente due anni fa, al momento attuale non esiste una libreria pubblica per l'impiego del framework, pertanto verrà sviluppata autonomamente nell'ambito di questa tesi.
* **MAPPINGS EXPLORER**: mette a disposizione un mapping tra le tecniche del dominio *Enterprise* del primo framework e le CVE conosciute fino al 2021 (limite dato dagli studi esistenti al momento della creazione del sistema in questione).
* **STI\_CYBER\_SECURITY\_MODEL\_V\_0\_1**: un modello linguistico pre-addestrato sul dominio di conoscenza della cybersecurity, utilizzato per ottenere dei vettori di embedding da cui calcolare la similarità coseno al fine di individuare una mappatura tra le le TTPs del framework ATT&CK e le CVE non presenti nel penultimo framework. Visto l’elevato numero esistenti di CVE e limitata quantità di TTPs, questo modello linguistico verrà utilizzato per ottenere la relazione tra CVE e tecniche, ma non viceversa.
* **NVDLib**: NIST National Vulnerability Database API Wrapper [], una API python che richiama la REST API fornita dal NIST per accedere al NVD, al fine di ottenere dati sulle CVE e CPE.

### Tipo di dati manipolato – STIX Object e dizionari

Per gestire e armonizzare efficacemente i dati provenienti da fonti diverse all'interno dello studio, è importante riconoscere la natura degli oggetti restituiti dal framework ATT&CK, rispetto ai dati estratti dai file JSON relativi alla matrice ATLAS e al mapping explorer. Gli oggetti forniti dal framework ATT&CK sono degli oggetti **STIX** (Structured Threat Information eXpression), che rappresentano un modo standardizzato per esprimere informazioni di intelligence sulle minacce informatiche. Gli oggetti STIX, espansi con altri attributi, che permettono di descrivere dettagliatamente e in maniera strutturata le informazioni su minacce, tattiche, tecniche e procedure (TTP), facilitando così lo scambio di informazioni di sicurezza tra sistemi e tra esperti del settore.

D'altro canto, i dati ottenuti dai file JSON relativi alla matrice ATLAS e al mapping explorer sono rappresentati sotto forma di semplici **dizionari** Python. Questi dizionari offrono una struttura flessibile per memorizzare e organizzare dati sotto forma di coppie chiave-valore, ma senza aderire a uno schema di rappresentazione standardizzato come nel caso degli oggetti STIX.

L'obiettivo è fondere i dati sugli attacchi delle matrici ATT&CK e ATLAS per una manipolazione uniforme, trasformando i dizionari in oggetti STIX per un accesso rapido ed efficiente ai dati, mantenendo le CVE come dizionari a causa del loro grande volume e assenza di informazioni a static-time.

Strutturazione package e directory

### Singleton

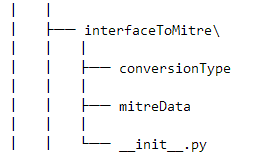
Per affrontare la sfida di gestire l'ampio volume di dati in questo studio, si è optato per l'adozione del pattern **Singleton** in diverse classi container. Al fine di implementare questo modello in modo efficiente, si è sviluppata una specifica funzione "*singleton*" per sfruttare la potente funzionalità dei decorator in Python (figura 9).

Il meccanismo alla base della funzione “*singleton*” prevede l'utilizzo di un dizionario per tracciare le istanze delle classi. Quando il costruttore di una classe decorata viene invocato per la prima volta, l'istanza viene creata normalmente e memorizzata in questo dizionario. Qualsiasi tentativo successivo di istanziare nuovamente la classe comporterà il recupero dell'istanza esistente dal dizionario, anziché la creazione di una nuova istanza.

  
Figura 9: implementazione del pattern Singleton in src/domain/Singleton.py

### Interfaccia per MITRE data

Per incapsulare efficacemente le funzionalità fornite dalle librerie sviluppate da MITRE e gestire la provenienza dei dati, è stata creato un package dedicato (figura 10), migliorando al contempo l'indipendenza del codice, la coerenza nell'utilizzo, la facilità di sostituzione, la semplicità di manutenzione e la capacità di eseguire test in modo efficace.

  
Figura 10: Strutturazione package */src/domain/InterfaceToMitre*

#### mitreData

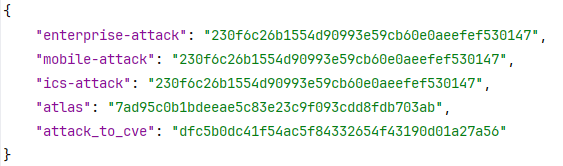
È un insieme di moduli che si occupano di ottenere, gestire gli aggiornamenti e fornire i dati provenienti dai vari framework, librerie esterne e modelli linguistici utilizzati, contiene vati sub-package (figura 11).

Figura 11: Strutturazione package   
*/src/domain/InterfaceToMitre/mitreData*

##### Fetch Data

Si tratta di un **modulo** **funzionale** integrato nel sistema che è preposto alla **verifica** dell'attualità **dei dati** conservati nella sottocartella "*files*". Questa verifica procede attraverso il confronto del codice hash dell'ultima commit realizzata sul branch principale del repository GitHub, da cui i dati originano, con il codice hash memorizzato al momento del download nel file “*local-hashes*” (figura 12), per ogni sorgente di dati.

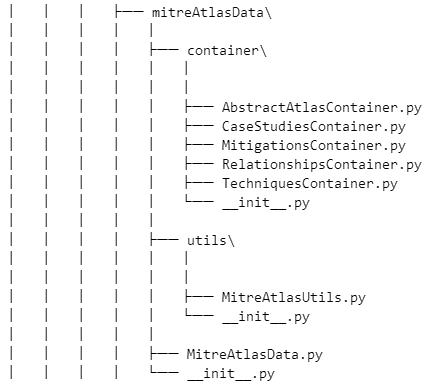
Nel caso in cui il dispositivo in uso non disponga di una connessione Internet, il software rimarrà operativo purché i dati siano stati precedentemente scaricati almeno una volta.

****  
Figura 12: Contenuto del file   
*src/domain/interfaceToMitre/mitreData/files/local-hashes.json*

##### Mitre Atlas Data

Il package *mitreAtlasData* (figura 13)è un insieme di moduli, il cui accesso esterno è regolato della classe progettata specificamente per estrarre e rendere disponibili i dati contenuti nel file "*atlas.json*", consentendo la loro manipolazione in tempo reale. Questa classe è stata sviluppata su misura per questo sistema, ispirandosi alla struttura e alla funzionalità della classe preesistente **MitreAttackData**. L'obiettivo era garantire che i dati ottenuti fossero in un formato STIX, uniforme e compatibile al framework ATT&CK facilitando così l'integrazione e la manipolazione efficace delle informazioni durante l'esecuzione del programma.

La classe in oggetto interagisce con degli oggetti presenti nel sub-package *container*, specificamente istanze singleton di classi progettate per recuperare i dati dai file JSON. Questi container fungono da intermediari dedicati all'acquisizione e alla gestione delle informazioni, diminuendo le richieste di lettura del file.

  
Figura 13: Strutturazione package  
*src/domain/InterfaceToMitre/mitreData/mitreAtlasData*

##### Mitre ATT&CK to CVE

Il package in questione (figura 14) si dedica a offrire un punto di accesso centralizzato per l'acquisizione di dati relativi alla correlazione tra le Common Vulnerabilities and Exposures (CVE) e il framework ATT&CK. Questo legame tra le vulnerabilità identificate (CVE) e le tattiche, tecniche e procedure (TTP) documentate nell'ATT&CK può essere stabilito seguendo due approcci distinti.

Nel caso in cui il CTID (Cyber Threat Intelligence ID) disponga di una mappatura esistente attraverso il framework MAPPINGS EXPLORER, la relazione verrà direttamente recuperata dal file "attack\_to\_cve.json", ottenendo il *mitre id*  degli attacchi correlati;

Qualora il CVE ID ricercato non risulti presente all'interno del file JSON, verrà eseguito un processo compensativo, il sistema procederà confrontando la descrizione della vulnerabilità specifica con quelle di ciascuna tecnica ATT&CK attraverso l'impiego di un LLM che implementino il meccanismo di sentence similarity. Al fine di individuare il miglior modello disponibili sono stati testai vari Sentence Similarity Model (**SSM**), l’unico a dare risultati soddisfacenti è denominato **sti\_cyber\_security\_model\_V\_0\_**. L'obiettivo è identificare quelle tecniche che mostrano una similarità “abbastanza elevata” per poter definire le tali tecniche correlate alla CVE ricercata.

Per stabilire un valore di soglia appropriato per la similarità coseno che indichi una relazione significativa tra una tecnica di attacco e una CVE, è stato condotto un'analisi su un ridotto dataset di XXX CVE precedentemente mappate dal MITRE. L'obiettivo è comprendere quanto efficacemente la similarità coseno rifletta le relazioni documentate di tipo "exploitation-technique" tra le descrizioni delle tecniche di attacco e delle CVE corrispondenti. Durante questa analisi sono stati calcolati i seguenti parametri:

* **Media Totale delle Similarità Ottenute**: Questo valore rappresenta la media delle similarità coseno calcolate tra le descrizioni delle tecniche di attacco e delle CVE, fornendo un'indicazione generale del livello di similarità nel dataset.
* **Numero di Falsi Negativi (FN)**: Si riferisce al numero di casi in cui le tecniche di attacco, pur essendo effettivamente correlate a una CVE secondo il mapping di MITRE, hanno mostrato una similarità coseno inferiore alla soglia stabilita. Questi casi indicano situazioni in cui il modello potrebbe non riconoscere una relazione valida a causa di una soglia troppo elevata.
* **Percentuale di Falsi Negativi**: Questa metrica esprime i falsi negativi come percentuale del totale delle mappature analizzate, offrendo una visione più chiara dell'impatto dei falsi negativi sulle performance generali del modello.
* **Numero di Falsi Positivi (FP)**: Questo parametro conta le istanze in cui tecniche di attacco non mappate con una CVE hanno presentato una similarità coseno superiore alla soglia scelta. Questi risultati possono indicare un'eccessiva sensibilità del modello, che identifica erroneamente relazioni non documentate come significative.
* **Percentuale di Falsi Positivi**: Simile alla metrica dei falsi negativi, questa percentuale rappresenta i falsi positivi in relazione al totale delle valutazioni effettuate, offrendo un'ulteriore dimensione di valutazione dell'accuratezza del modello.

Questi parametri sono stati fondamentali per affinare la scelta della soglia di similarità coseno, mirando a un equilibrio ottimale tra evitare falsi negativi (mancare relazioni reali) e minimizzare falsi positivi (evitare relazioni inesistenti), in modo da massimizzare sia la precisione sia la copertura del modello utilizzato per l'analisi delle relazioni tra CVE e tecniche di attacco.

La **media** della similarità ottenuta dalle XXX similarità cercate è uguale a **YYY**, il che sembra indicare come threshold un valore di circa YYY.

Lo studio ha evidenziato che una soglia di similarità minima pari a **0.50** fornisce (tabella 1)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Media totale** | **n° FN** | **% FN** | **N° FP** | **% FP** |
|  |  |  |  |  |

Tabella 1: Parametri ottenuti per similarità coseno = 0.50

Lo studio ha evidenziato che una soglia di similarità minima pari a **0.60** fornisce (tabella 2)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Media totale** | **n° FN** | **% FN** | **N° FP** | **% FP** |
|  |  |  |  |  |

Tabella 2: Parametri ottenuti per similarità coseno = 0.60

Lo studio ha evidenziato che una soglia di similarità minima pari a **0.70** fornisce (tabella 3)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Media totale** | **n° FN** | **% FN** | **N° FP** | **% FP** |
|  |  |  |  |  |

Tabella 3: Parametri ottenuti per similarità coseno = 0.70

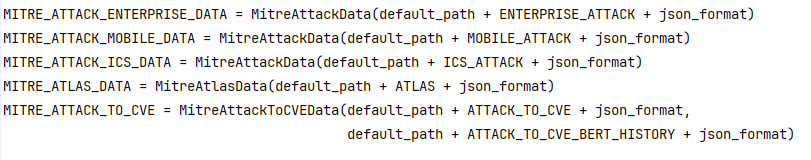
Tramite la classe singleton **SentenceSimilarityModel** è possibile interagire con il modello semantico scelto. Questo permette di generare una nuova mappatura, la quale verrà successivamente salvata nel file "attack\_to\_cve\_ssm\_history.json". Di conseguenza, le ricerche future della stessa vulnerabilità risulteranno significativamente più veloci, grazie alla disponibilità immediata della correlazione precedentemente determinata.

Figura 14: Struttura del package *src/domain/InterfaceToMitre/mitreData/mitreAttackToCVE*

##### Mitre Data

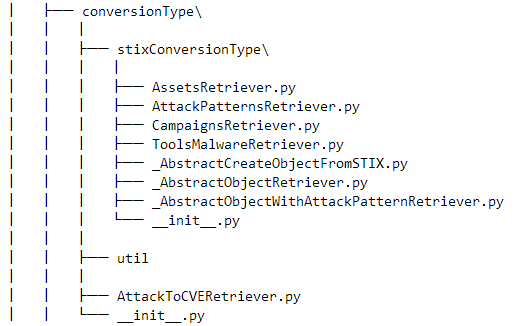
Si tratta di un componente del software che svolge il ruolo di **interfaccia** ai “**dati** **raw**” provenienti dai file JSON (figura 15). Mette a disposizione quattro variabili statiche che rappresentano i diversi dataset utilizzati relativi al dominio della sicurezza informatica, come specificato di seguito:

* **MITRE\_ATTACK\_ENTERPRISE\_DATA**: carica i dati dell'ATT&CK Enterprise da file JSON.
* **MITRE\_ATTACK\_MOBILE\_DATA**: fornisce l'accesso ai dati dell'ATT&CK per il contesto mobile.
* **MITRE\_ATTACK\_ICS\_DATA**: rende disponibili i dati dell'ATT&CK per i sistemi di controllo industriale (ICS).
* **MITRE\_ATLAS\_DATA**: fornisce i dati della matrice ATLAS per sistemi in cui è presente una componente di AI.
* **MITRE\_ATTACK\_TO\_CVE**: offre un ponte tra i dati di ATT&CK e le vulnerabilità specifiche (CVE), permettendo una mappatura diretta tra le tecniche di attacco e le vulnerabilità note.

Figura 15 Contenuto del modulo *src/domain/interfaceToMitre/mitreData/MitreData*

#### Conversion Type

È un insieme di moduli (figura 16) che richiamano le interfacce di comunicazione con i framework e librerie (figura 15), in modo da gestire e modificare il formato dei “dati raw” qualora necessario. Utilizzando questo approccio, si migliora anche la facilità di manipolazione dei dataset, poiché si accede direttamente a oggetti Python anziché a file JSON complessi. In un file JSON, per recuperare un singolo dato, potrebbe essere necessario navigare attraverso diversi livelli gerarchici, rendendo il processo più macchinoso. La conversione dei dati in oggetti Python semplifica notevolmente questo processo, migliorando la manutenibilità del sistema e rendendo il codice più intuitivo e facile da gestire. Questa strutturazione più diretta e accessibile dei dati contribuisce a ridurre gli errori e a facilitare le future estensioni e modifiche del codice.

  
Figura 16: Struttura del package  
*src/domain/InterfaceToMitre/conversionType*

##### STIX Conversion Type

È il modulo che si occupa di recuperare gli oggetti STIX espansi, tramite le interfacce **MITRE\_ATTACK\_ENTERPRISE\_DATA**, **MITRE\_ATTACK\_MOBILE\_DATA**, **MITRE\_ATTACK\_ICS\_DATA** e **MITRE\_ATLAS\_DATA** e convertirli in oggetti **MySTIXObject** definiti nell’ambito di questo studio, al fine di mantenere a run-time la correlazione tra gli oggetti **AttackPattern**[[12]](#footnote-13), **Campaign**[[13]](#footnote-14), **CourseOfAction**[[14]](#footnote-15), **Tool**[[15]](#footnote-16)e **Malware**[[16]](#footnote-17)(i precedenti due oggetti non vengono distinti nei framework MITRE e prendono il nome di **Software**), senza dover effettuare molteplici ricerche per ottenere la relazione tra essi.

##### Attack to CVE Retriever

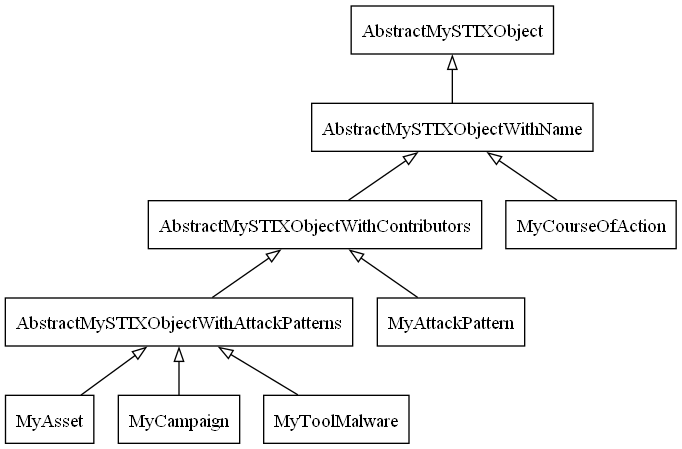
Questa classe è stata specificamente sviluppata per rendere disponibili i "dati raw" acquisiti mediante l'interfaccia **MITRE\_ATTACK\_TO\_CVE**. Al fine di utilizzare un unico modulo centralizzato come unico punto di accesso ai dati, i quali sono immediatamente pronti per essere utilizzati.

### Business

Il modulo business del dominio è progettato per stabilire e gestire gli oggetti che saranno impiegati nella memorizzazione e nel trattamento in tempo reale delle informazioni legate ad AttackPattern, Campaign, Tool, Malware, Asset e CourseOfAction, secondo quanto delineato dai vari framework MITRE, mantenendo a run-time le correlazioni tra gli oggetti.

#### MySTIXObject

Il modulo include una ridefinizione degli oggetti STIX (figura 17) per preservare, durante l'esecuzione, le relazioni tra AttackPattern e CourseOfAction e le associazioni tra Campaign, Tool, Malware, Asset i relativi AttackPattern di riferimento.

  
Figura 17: Ereditarietà delle classi MySTIX

##### Ottimizzazione della memoria e tempi di accesso

Data l'ampia quantità di oggetti gestiti in tempo reale e con l'obiettivo di ottimizzare l'uso della memoria e ridurre i tempi di accesso alle strutture dati, è stato adottato l'uso delle **dataclass** di Python. Queste strumentazioni offrono un modo efficace per implementare oggetti immutabili, mediante l'attributo *frozen*, e per ottimizzare l'utilizzo della memoria attraverso l'attributo *slots*. L'impiego delle dataclass consente di definire classi con una sintassi più semplice e pulita, garantendo al contempo un accesso rapido ai dati e una gestione della memoria più efficiente, aspetti fondamentali in contesti dove il volume di dati è elevato e le performance sono critiche.

#### Attack Phase

Si tratta di un'enumerazione progettata per amalgamare e stabilire una sequenza di esecuzione per le tattiche delineate nei framework ATT&CK e ATLAS. L'obiettivo è di delineare una successione logica nell'esecuzione degli attacchi, basandosi sul concetto della cyber kill chain. Attraverso l'analisi dell'ordine in cui le tattiche si manifestano nei suddetti framework, è stata ricreata la cyber kill chain, che segue la sequenza delle operazioni come individuato nei framework ATT&CK e ATLAS, riflettendo così una strutturazione meticolosa delle fasi dell'attacco in relazione alle metodologie cyber:

1. **Reconnaissance**:
   1. Reconnaissance (Enterprise, Atlas)
2. **Weaponization**:
   1. Resource Development (Enterprise, Atlas)
3. **Delivery**:
   1. Initial Access (Enterprise, Mobile, ICS, Atlas)
   2. ML Model Access (Atlas)
4. **Exploitation**:
   1. Execution (Enterprise, Mobile, ICS, Atlas)
5. **Installation**:
   1. Persistence (Enterprise, Mobile, ICS, Atlas)
   2. Privilege Escalation (Enterprise, Mobile, ICS, Atlas)
   3. Defense Evasion (Enterprise, Mobile, Atlas)
   4. Evasion (ICS)
6. **Command** **& Control**:
   1. Credential Access (Enterprise, Mobile, Atlas)
   2. Discovery (Enterprise, Mobile, ICS, Atlas)
   3. Lateral Movement (Enterprise, Mobile, ICS)
   4. Command and Control (Enterprise, Mobile, ICS)
   5. Collection (Enterprise, Mobile, ICS, Atlas)
   6. Inhibit Response Function (ICS)
7. **Action**:
   1. Impair Process Control (ICS)
   2. ML Attack Staging (Atlas)
   3. Exfiltration (Enterprise, Mobile, Atlas)
   4. Impact (Enterprise, Mobile, ICS, Atlas)

### Container

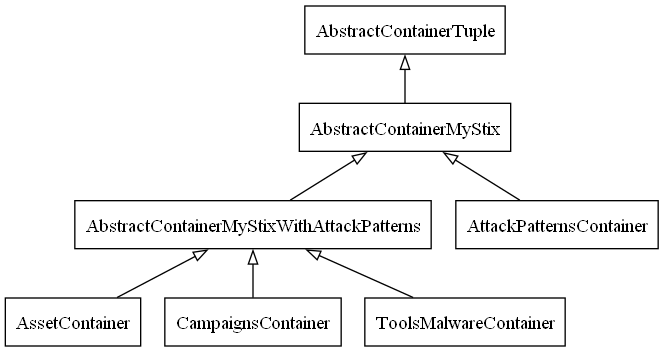
Questo package contiene le classi singoletto utilizzate per accedere ai dati MySTIX e alla relazione tra CVE e gli oggetti MyAttackPattern.

#### My STIX Container

Il modulo in questione include la definizione di classi singleton progettate per agevolare l'accesso a oggetti ampiamente utilizzati all'interno del sistema (figura 18). Queste classi giocano un ruolo fondamentale nell'organizzazione e nella gestione delle informazioni derivate dai framework ATT&CK e ATLAS, attraverso l'implementazione di meccanismi specifici:

* **Ricerca degli Oggetti**: Le classi consentono il ritrovamento di oggetti basati sui loro identificativi unici—sia esso un STIX ID, un MITRE ID o semplicemente il nome—presenti nei framework ATT&CK e ATLAS. Questa funzionalità è essenziale per navigare efficacemente all'interno della vasta quantità di dati e per recuperare informazioni specifiche con precisione.
* **Esplorazione delle Relazioni**: È stato sviluppato un approccio per analizzare le connessioni tra gli attack pattern e identificare potenziali tecniche correlate a una di queste. In particolare, è stato introdotto il metodo *get\_related\_attack\_patterns\_by\_attack\_pattern\_id* nella classe *AttackPatternsContainer*. Questo metodo si focalizza sull'identificazione degli attack pattern coinvolti in campagne o software noti, assumendo che le tecniche legate a queste entità siano in qualche modo connesse all'attack pattern di interesse. Implementando una verifica incrociata tra le diverse entità, il sistema è in grado di delineare un quadro complesso delle interrelazioni tra le tecniche di attacco.

Sulla base delle funzionalità descritte in precedenza e dell'analisi sull'ordine potenziale di esecuzione delle tattiche offensive, sono stati sviluppati due metodi cruciali. Questi metodi consentono di generare dizionari che indicano, rispettivamente, **i possibili attack pattern che potrebbero manifestarsi in futuro** (*get\_futured\_attack\_patterns\_grouped\_by\_phase*) e **quelli** **che potrebbero già essere stati attuati in passato** (*get\_probably\_happened\_attack\_patterns\_grouped\_by\_phase*), a seguito dell'attacco specifico oggetto di indagine. Questa distinzione tra attacchi futuri potenziali e passati permette di adottare un approccio proattivo nella difesa, anticipando le mosse degli avversari, e al contempo di analizzare retrospettivamente gli eventi di sicurezza per individuare pattern o lacune nella protezione. Il risultato è una visione più completa e dinamica della sequenza di attacchi, arricchendo la comprensione delle minacce e fornendo insight preziosi per la pianificazione di strategie di difesa ottimali.

  
Figura 18: Ereditarietà delle classi container

#### Attack to CVE Container

È la classe container che ha il compito di recuperare la relazione tra le CVE e gli attack pattern al fine di fornire l’identificativo della CVE o un report CTI al sistema ed ottenere informazioni relative allo stato di sicurezza dell’organizzazione tramite la consapevolezza di possibili tecniche che possano essere avvenute o che possano avvenire. Come spiegato precedentemente se la tecnica non è stata mappata nel framework MAPPINGS EXPLORER del CTID verrà utilizzato il modello linguistico sti\_cyber\_security\_model\_V\_0\_1 per trovare le relative tecniche connesse alla CVE, con una similarità coseno maggiore o uguale a 0.5, salvando tali informazioni per rendere la prossima ricerca con gli stessi parametri notevolmente più rapida.

# Bibliografia

[1] *Cisco* (2022).   
https://www.cisco.com/c/it\_it/products/security/what-is-cybersecurity.html

[2] *Wikipedia* (2024, Marzo 11). https://it.wikipedia.org/wiki/Internet\_delle\_cose

[3] *Cisco* (2023).   
https://www.learncisco.net/courses/iins/common-security-threats/information-security-and-common-threats.html

[4] *Check Point* (2023, Luglio). https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

[5] *Statista* (2024, Febbraio 23). https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/

[6] Statista (2024, Febbraio 22). https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[7] *Agenda Digitale Eu* (2024, Gennaio 25). https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/

[8] Tauran Yadav, Rao Arvind Mallari (2016, Giugno 10).  
Technical Aspect of Cyber Kill Chain

[9] Erico M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. Lockheed Martin Corportation (2015, Settembre 12).   
Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain

[10] Blake E. Storm, Joseph A. Battaglia, Michael S. Kemmerer, William Kupersanin, Douglas P. Millar, Craig Wampler, Sean M. Whitley, Ross D. Wolf (2017, Giugno).  
Finding Cyber Threats With ATT&CK-Based Analytics

[11] Mitre ATLAS (2021, 17 Febbraio)  
https://atlas.mitre.org/

[12] Cyber Conflict Istitute (2022 Giugno)  
https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/Viasat

[13] Nicolò Boschetti, Nathaniel G. Gordon, Gregory Falco  
Space Cybersecurity Lessons Learned from The Viasat Cyberattack

[14] Wikipedia (2024).  
https://en.wikipedia.org/wiki/Common\_Vulnerabilities\_and\_Exposures

[15] Wikipedia (2024).  
https://en.wikipedia.org/wiki/Common\_Weakness\_Enumeration

[16] Kevin Poireault, (2023, Dicembre 28)  
https://www.infosecurity-magazine.com/news-features/navigating-vulnerability-maze-cve/

[17] Center for Threat-Informed Defense (2012, Ottobre 21)  
https://center-for-threat-informed-defense.github.io/mappings-explorer/about/methodology/cve-methodology/

[18] Mitre ATT&CK (2020, 16 Dicembre)  
https://github.com/mitre-attack/mitreattack-python/

[19] Basel Abdeen , Ehab Al-Shaer , Anoop Singhal , Latifur Khan, Kevin

Hamlen (2023, 15 Aprile)  
SMET: Semantic Mapping of CVE to ATT&CK and its Application to Cybersecurity

[20] Wikipedia (2013, 20 Giugno)  
https://it.wikipedia.org/wiki/Coseno\_di\_similitudine

[21] Wikipedia (2014, 27 Settembre)  
https://en.wikipedia.org/wiki/Word\_embedding

[22] Wikipedia (2008, 7 Gennaio)  
https://en.wikipedia.org/wiki/Cosine\_similarity

[23] vehemont (2021, 15 Ottobre)  
https://github.com/vehemont/nvdlib

1. Acronimo del neologismo **Internet of Things**. [↑](#footnote-ref-2)
2. Si riferisce a uno stile di vita reso più efficiente e comodo attraverso l'uso di dispositivi connessi e tecnologie intelligenti. [↑](#footnote-ref-3)
3. Colui che svolge l’attacco. [↑](#footnote-ref-4)
4. Combinazione di exploit (es. per attacchi a sistemi web questi coprono l’eventualità di utilizzo di CVE in base ai di differenti Browser esistenti) [↑](#footnote-ref-5)
5. Coloro che hanno il compito di difendere, prevenire e identificare gli attacker [↑](#footnote-ref-6)
6. Gruppo di attacker con intenzioni malevole [↑](#footnote-ref-7)
7. Avere una conoscenza dettagliata di come una componente/sistema è sviluppato (conoscere cosa c’è dentro la scatola) [↑](#footnote-ref-8)
8. Ramo della MITRE Corporation [↑](#footnote-ref-9)
9. Rappresenta la "lunghezza" del vettore nello spazio vettoriale, ovvero la distanza dal punto di origine [↑](#footnote-ref-10)
10. Secondo semestre [↑](#footnote-ref-11)
11. **Computer Security Incident Response Team**, gruppo di sicurezza governativo con il compito di regolamentare le cooperazioni con il settore privato nella sfera della cybersicurezza. [↑](#footnote-ref-12)
12. Oggetto STIX che identifica una tecnica [↑](#footnote-ref-13)
13. Oggetto STIX che identifica le campagne [↑](#footnote-ref-14)
14. Oggetto STIX che identifica le mitigazioni [↑](#footnote-ref-15)
15. Oggetto STIX che identifica i tool [↑](#footnote-ref-16)
16. Oggetto STIX che identifica i malware [↑](#footnote-ref-17)