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 PREVENZIONE DEL RISCHIO DIGITALE

Relatore:

Prof.ssa Vita Santa Barletta

Laureando:

Nicola Balzano

Anno Accademico 2023/2024

INDICE

Abstract

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 del presente studio, che esplora come la cybersecurity è diventata una materia indispensabile per proteggere i dati e le infrastrutture che sostengono la nostra società. L'uomo sta andando incontro all'evoluzione, giorno dopo giorno. 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** (**TTPs**) 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.

Per ottenere un **vantaggio significativo** contro gli agenti di minaccia, bisognerebbe conoscere ad ogni possibile tecnica di attacco quali sono quelle che possano avvenire successivamente o che possano essere già avvenute.

In questo contesto, l'**obiettivo** primario del presente studio è esattamente quello di esplorare e delineare l'importanza di un approccio proattivo nella sicurezza informatica, attraverso lo sviluppo di un sistema che permetta un'analisi quantitativa e dettagliata delle strategie offensive e difensive, insieme all'**implementazione di soluzioni innovative per la prevenzione e il rilevamento di ogni possibile minaccia** conosciuta nella CTI, anticipando le possibili azioni che un attacker può compiere in ogni fase della Cyber Kill Chain e correlando ad ogni possibile vulnerabilità le tecniche utilizzabili.

CAPITOLO I

Introduzione

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

1.1 Internet of Things – Un mondo interconnesso

Il concetto dell'**Internet delle Cose** [1] (**IoT**[1]) è alla base della vita smart[2] che l'uomo vive ogni giorno. Esso 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**,

---

[1] Acronimo del neologismo **Internet of Things** anche nota come **Internet of Everythings** (**IoE**).

[2] Si riferisce a uno stile di vita reso più efficiente e comodo attraverso l'uso di dispositivi connessi e tecnologie intelligenti.

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.

1.2 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.

1.3 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** (**CKC**) [8] (figura 1).

È fondamentale analizzare e capire in dettaglio la CKC 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 i quali un aggressore pianifica ed esegue un attacco.

Figura 1: Fasi della Cyber Kill Chain

Le fasi di cui è composta la CKC 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:
    a. ***Passiva***: utilizza metodi che non permettono all'individuo/organizzazione target di individuare le azioni di ricognizione in corso (es. Domain Names, whois, Social Network).
    b. ***Attiva***: permette di ottenere un profilo del target più specifico ma potrebbe mettere in allerta la vittima (es. Port scanning and Services).
2. **Weaponization**: ha lo scopo di progettare il metodo con cui agire, tramite le informazioni ottenute precedentemente, progettando e sviluppando due componenti:

a. ***RAT***: *Remote Access Tool*, la parte di software che permette di ottenere l'accesso quando viene eseguita sul sistema target, solitamente anche chiamata *payload of cyber-weapon*.

b. ***Exploit***: lo script che permette di eseguire il RAT utilizzando vulnerabilità dei sistemi/software target, tramite l'utilizzo di *CVE*[3].

3. **Delivery**: è la parte critica della catena per un attacker[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**: 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*[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.

---

[3] Common Vulnerabilities and Exposures

[4] Colui che svolge l'attacco.

[5] Combinazione di exploit (es. per attacchi a sistemi web questi coprono l'eventualità di utilizzo di CVE in base ai differenti Browser esistenti)

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:
    a. ***Struttura Centralizzata***: classica *struttura client-server*, la limitazione consiste nel numero di risorse hardware/software disponibili nel *C2 Server*.
    b. ***Struttura Decentralizzata***: prevede l'utilizzo della modalità di *comunicazione peer-to-peer*, la quale permette alta scalabilità e tolleranza verso gli errori di trasmissione.
    c. ***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).

1.4 APT e Indicatori

Per via dell'avanzamento delle tecnologie difensive del **blue team**[6], anche il **red team**[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 degli 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)

---

[6] Coloro che hanno il compito di difendere, prevenire e identificare gli attacker

[7] Gruppo di attacker con intenzioni malevole

- **Comportamentali**: maggiormente utilizzati, sono collezione di indicatori atomici e calcolati in combinazione logica tra loro.

1.5 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 anch'esso dalla **MITRE Coporation**, ormai da anni queste sono uno dei principali metodi di identificazione univoco delle minacce su software proprietario.

La caratteristica distintiva delle CVE è l'assegnazione di un identificativo unico, o CVE-ID, ad ogni vulnerabilità registrata. Originariamente, dal loro inizio nel 1999, i CVE-ID 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 specifiche. 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 ai **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, quest'ultimo inoltre sono correlate al **MITRE ATT&CK Framework** (figura 2).

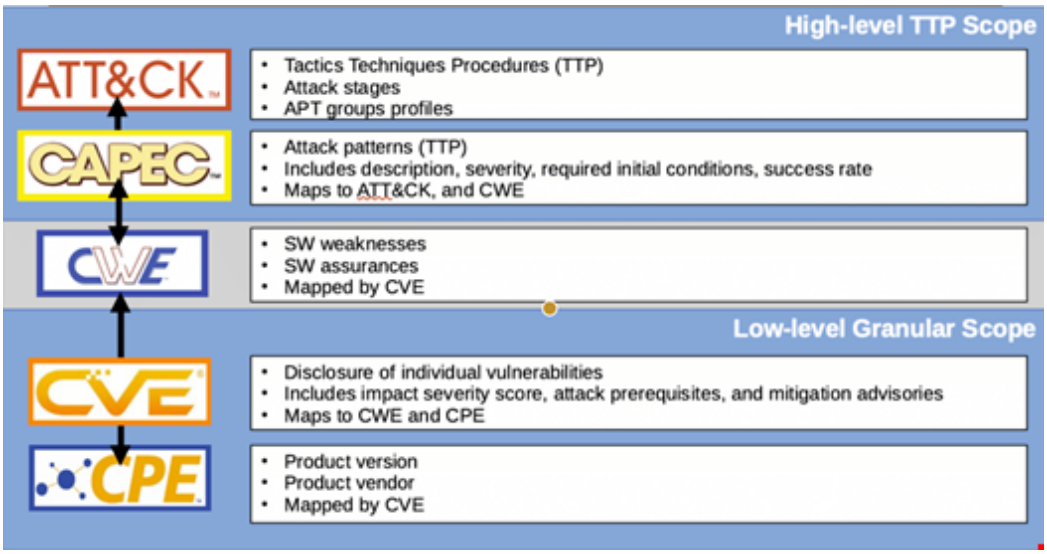

Figura 2: Correlazione tra CPE-CVE-CWE-CAPEC-ATT&CK [16]

CAPITOLO II

Stato dell'Arte

2.1 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 gli 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 che possono soffrire in casi di attacchi informatici (**asset**);
- tool/malware frequentemente usati dal red team per compiere azioni malevole (**software**).

Il framework mette a disposizione 3 matrici in modo da suddividere l'ambiente in cui gli attacchi possano avvenire: ***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, ad un pericolo o ad 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 ed 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. Questo strumento offre una piattaforma interattiva e facilmente navigabile che permette agli analisti di sicurezza, ai ricercatori ed 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. Il Navigator, inoltre, 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).

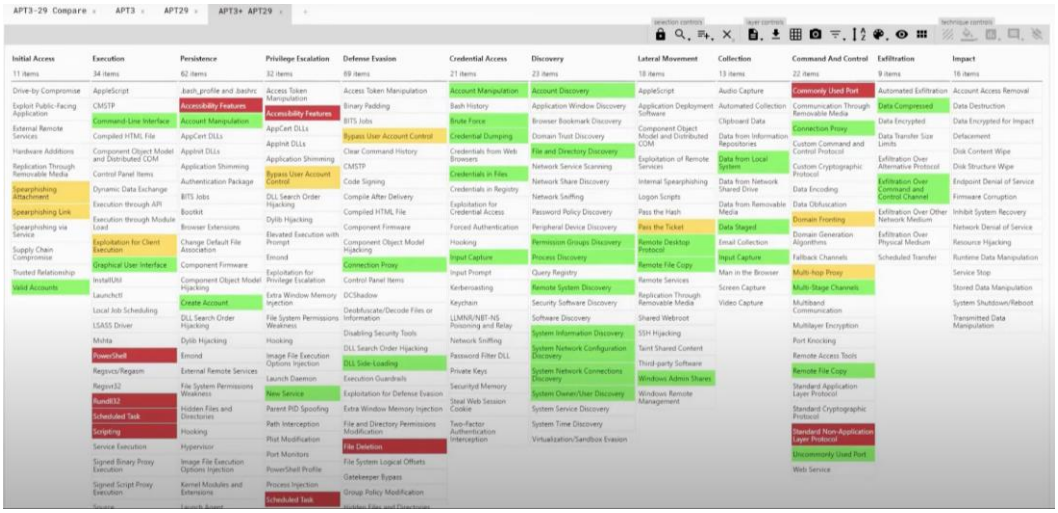

Figura 3: Esempio di utilizzo del MITRE ATT&CK Navigator studio dell'unione di APT3, APT29, APT3+APT29

2.2 MITRE ATLAS – Nuove tecnologie e nuove minacce

Con l'ascesa e l'espansione delle tecnologie dell'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*[8] del sistema target per personalizzare l'attacco.
- Exfiltration
- Impact

[8] Avere una conoscenza dettagliata di come una componente/sistema è sviluppato (conoscere cosa c'è dentro la scatola)

2.3 Mappatura Vulnerabilità – MITRE TTPs

Al fine di raggiungere l'obiettivo del presente studio bisogna trovare un approccio per ottenere la relazione tra le MITRE TTPs e le possibili vulnerabilità, in modo da approfondire e analizzare l'impatto di ogni vulnerabilità nel proprio ambiente di sviluppo tramite un'analisi quantitativa.

2.3.1 Mappings Explorer

Per approfondire lo studio sugli impatti che ogni vulnerabilità, identificata tramite una CVE, può avere su un sistema informatico, la **CTID** (Center for Threat-Informed Defense) ha continuato a sviluppare un framework della **MITRE ENGENUITY**[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 MAPPINGS EXPLORER 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;

[9] Ramo della MITRE Corporation

- **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 o non è possibile delinearlo.

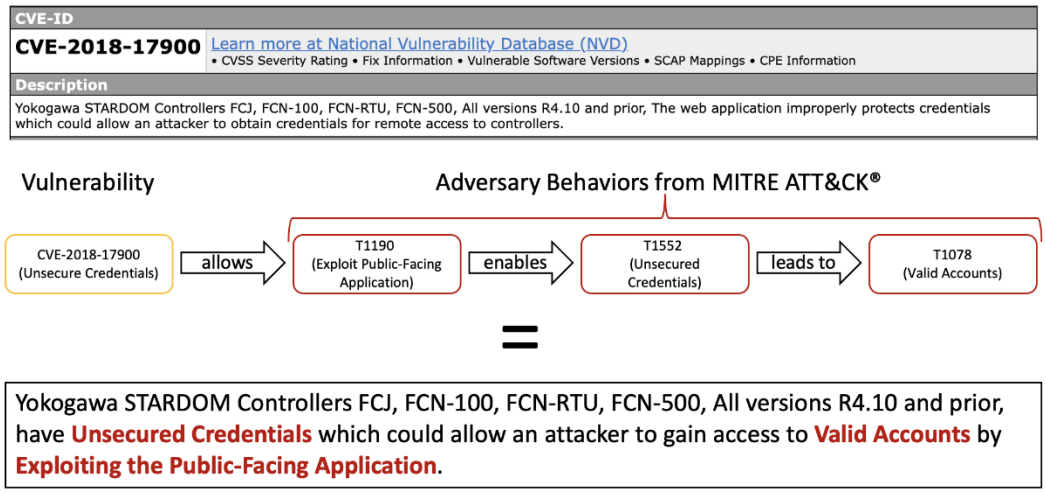

Figura 4: Esempio di come una CVE è relazionata al framework ATT&CK [17]

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 all'anno 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 verranno impiegate anche altre tecniche per ottenere la medesima relazione tra vulnerabilità e attack patterns MITRE.

2.3.2 Altri metodi di relazione tra Vulnerabilità e TTPs

Molteplici sono gli studi che hanno cercato di trovare una soluzione nel colmare il divario tra l'ambito delle TTPs e quello delle vulnerabilità.

Di seguito vengono presentati i più recenti studi degni di nota nel contesto descritto.

2.3.2.1 Mapping CVEs and ATT&CK Framework TTPs: An Empirical Approach

Un approccio empirico [16] per mappare le CVE con gli attack patterns del framework ATT&CK si basa sulla natura relazionale che vi è tra queste informazioni.

Come descritto precedentemente, una CVE è correlata a zero, una o più CWEs, a sua volta correlata a zero, uno o più CAPECs, a sua volta correlata a zero, uno o più attack patterns del framework ATT&CK. Ripercorrendo questa catena di relazioni è possibile quindi, data una determinata vulnerabilità CVE o CWE, ottenere la relazione di essa con il framework MITRE ATT&CK (figura 2).

Considerando che ATT&CK si evolve molte velocemente ed è nato 5 anni dopo il catalogo CAPEC, debuttato a sua volta anni dopo la nascita del sistema delle CWE, lo **svantaggio** dell'approccio presentato sta nel fatto che non sempre vi sono relazioni tra CVE e CWEs, tra CWE e CAPECs o tra CAPEC e MITRE TTPs, quindi non è

sempre possibile ottenere la relazione finale tra vulnerabilità e MITRE TTPs.

2.3.2.2 SMET - Semantic Mapping of CVE to ATT&CK and its Application to Cyber Security

SMET [24] è un nuovo strumento che utilizza un modello denominato ATT&CK BERT per mappare automaticamente le voci di CVE alle tecniche di ATT&CK in base alla similarità testuale. ATT&CK BERT è un **modello di similarità** tra frasi, o "**sentence similarity model**", un modello di ML utilizzato nel campo dell'elaborazione del linguaggio naturale (**NLP**) per determinare quando una vulnerabilità è correlata ad una TTP. Il modello risultante è ottenuto tramite il fine-tuning del modello noto come BERT[10].

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, catturano il contesto e il significato semantico delle entità linguistiche trasformando il testo in un

[10] Bidirectional Encoder Representations from Transformers, modello di ML nell'ambito del NLP, sviluppato da Google.

formato che può essere facilmente processato dai modelli di machine learning. I vettori risultanti dall'utilizzo di tale modello semantico permettono ai ricercatori di studiare la similarità tra 2 testi, tramite vari modi, nello studio in questione [25] viene utilizzata 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[11].

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

$$\text{Similarità Coseno} = \frac{A \cdot B}{\| A \| \cdot \| B \|}$$

Dove:

- $A \cdot B$ rappresenta il prodotto scalare dei vettori A e B
- $\| A \| \cdot \| B \|$ sono le magnitudini dei vettori A e B, calcolate come $\sqrt{\sum a_i^2}$ e $\sqrt{\sum b_i^2}$ rispettivamente dove a_i e b_i 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,

[11] Rappresenta la "lunghezza" del vettore nello spazio vettoriale, ovvero la distanza dal punto di origine.

- 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).

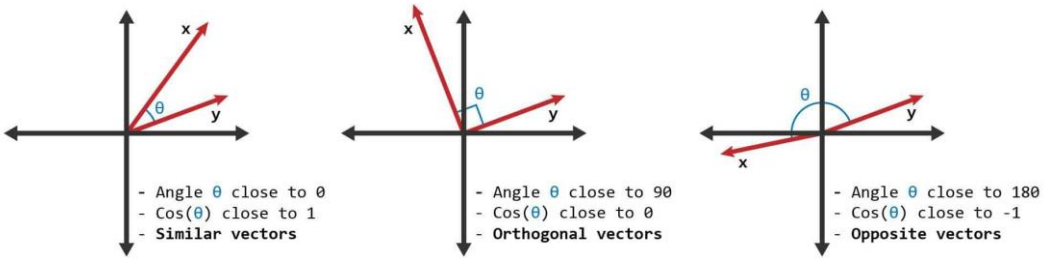

Figura 5: rappresentazione grafica della similarità coseno tra due vettori

Il modello in questione però è addestrato solo su un **dataset ridotto** di TTPs del framework **ATT&CK** e nessuna del framework ATLAS; inoltre vari test di studi [30] differenti dimostrano come questo LLM sia particolarmente impreciso quando gli si danno in input descrizioni come quelle dei noti APT, essendo così limitato non può essere utilizzato nello sviluppo di questo applicativo.

2.3.2.3 TRAM – Threat Report ATT&CK Mapper

TRAM (Threat Report ATT&CK Mapper) [25], sviluppato da MITRE Engenuity, è uno strumento che mira ad individuare le relazioni tra

un report testuale proveniente dalla community CTI e le TTPs (Tactics, Techniques, and Procedures) del framework MITRE ATT&CK utilizzando un modello di machine learning basato su BERT e un modello di Regressione Logistica[12]. Tuttavia, sebbene lo strumento sembri essere pratico, attualmente non offre un'API pronta per la produzione limitando la sua integrazione diretta con altri sistemi machine-to-machine. Anche se è possibile bypassare questa limitazione utilizzando tecniche di web scraping o ricreazione dei metodi di accesso alle informazioni finali, va notato che TRAM si basa su modelli di machine learning addestrati su report provenienti esclusivamente dalla CTI community, di conseguenza, non è in grado di analizzare descrizioni relative a CVE che risultano molto specifiche al software a cui si rivolgono, come invece richiesto nello studio in questione.

2.3.2.4 Threat action extraction using information retrieval

In un altro studio [28] è stato proposto un modello denominato **SecureBERT** per estrarre azioni di minaccia utilizzando tecniche di

[12] Modello di classificazione binaria, predice la probabilità che un'osservazione appartenga a una delle due classi utilizzando una funzione sigmoide per trasformare l'output in un valore compreso tra 0 e 1.

recupero delle informazioni. Per catturare le azioni di minaccia, questo studio utilizza vettori di parole, algoritmi di tagging e di filtraggio. La soluzione proposta genera automaticamente una lista di azioni di minaccia come base dell'ontologia; impiega una tecnica di estrazione delle minacce in due fasi e utilizza modelli di vettori di parole per l'estrazione di queste azioni. Tuttavia, questo lavoro etichetta i token in una frase con le loro categorie grammaticali utilizzando il part-of-speech tagging, ma non mantiene i legami grammaticali tra di essi, risultando quindi una semantica limitata e poco utile per collegare i testi di cybersicurezza molto complessi e prolissi.

2.3.2.5 TTPpredictor - CVE-driven attack technique prediction with semantic information extraction and a domain-specific language model

Nello studio in quesitone [26] è stato migliorato il modello precedentemente creato dai medesimi autori denominato SecureBERT (modello basato su BERT che utilizza il SRL[13]) [27], con il nuovo nome di **TTPpredictor**.

[13] Semnatic Role Labeling, processo che assegna etichette a parole o frasi in una frase, indicando il loro ruolo semantico nella frase.

Gli autori affermano di aver ottenuto un'accurancy[14] di circa il 98% e un F1-score tra il 95% e 98%.

Tuttavia, nonostante l'efficacia di TTPpredictor, questo strumento non può essere utilizzato per lo studio in questione poiché non considera le CWE e le TTPs della matrice ATLAS, tantomeno potrà essere testato visto che non sembra essere[15] di pubblico dominio.

2.3.2.6 ExAction: Automatically extracting threat actions from cyber threat intelligence report based on multimodal learning

In questo paper [29], gli autori presentano un meccanismo per estrarre automaticamente azioni di minaccia dai rapporti APT e produrre TTPs. Vengono estratte le azioni di minaccia dai rapporti APT utilizzando un estrattore basato su BERT-BiLSTM-CRF. Viene usata una tecnica per estrarre relazioni tra entità collegando le entità in modo contestuale e semantico. Questo approccio però ha

[14] Metrica che misura quanto spesso il modello predice correttamente il risultato.

[15] È il processo di contrassegnare una parola in un testo come corrispondente a una parte particolare del discorso, in base sia alla sua definizione che al suo contesto.

capacità limitate di estrazione delle azioni a causa della sua eccessiva dipendenza dall'analisi semantica e del part-of-speech che non riesce a identificare correttamente i riferimenti dei pronomi. Inoltre questo studio non si estende al collegamento delle informazioni sulle vulnerabilità e sulle minacce, risultando così inutilizzabile per la risoluzione dell'obiettivo posto.

2.3.2.7 Automated threat report classification over multi-source data

Altri ricercatori [30] hanno sfruttato tecniche di elaborazione del linguaggio naturale per estrarre azioni degli aggressori da 18.257 documenti di rapporti di minacce generati da diverse organizzazioni e le hanno classificate automaticamente in tattiche e tecniche standardizzate. La mancanza di dati etichettati e formati di rapporti non standard sono le principali sfide che questo studio affronta utilizzando un approccio di correzione dei bias. In questo lavoro, dove le descrizioni testuali dei report vengono tokenizzate, viene calcolato il punteggio TF-IDF per ogni parola e vengono applicati diversi meccanismi di correzione dei bias per superare i formati non standard. Tuttavia come riportato, questo approccio mostra una precisione molto bassa, vicina al 60%, nella classificazione delle informazioni sulle minacce in tecniche ATT&CK quando si utilizzano rapporti di minacce comunemente usati come le note APT e i dataset Symantec come dati di test.

2.3.2.8 BRON

BRON [31] è un framework completo che combina più fonti pubbliche di informazioni su minacce e vulnerabilità informatiche ovvero MITRE's ATT&CK MATRIX, CWE, CVE e CAPEC. BRON mantiene tutte le voci e le relazioni, facilitando il tracciamento bidirezionale del percorso. Esso utilizza modelli di attacco per stabilire connessioni tra obiettivi di attacco, mezzi, vulnerabilità e configurazioni software e hardware mirate. Nonostante il grande database di informazioni sulle minacce raccolte in questo studio, questo dataset è inutilizzabile per addestrare modelli di classificazione CVE to TTPs perché l'etichettatura è troppo generale/astratta e non si orienta verso le specifiche CVE/CWE e tecniche MITRE.

2.3.2.9 Linking CVEs to mitre att&ck techniques

Un'altra soluzione [32] proposta da altri ricercatori promuove l'uso della tassonomia MITRE ATT&CK per mappare le CVE alle tecniche di attacco. Introducono un modello di rete neurale di embedding multi-head con etichettatura non supervisionata per automatizzare questo processo. In questo studio si afferma che arricchire le CVE con una base di conoscenza di strategie di mitigazione e scenari di attacco migliora il modello nella comprensione. La valutazione mostra la mappatura di molte CVE alle tecniche ATT&CK, ma le limitazioni, tra cui una copertura limitata di sole 17 tecniche e una piccola base di conoscenza, rendono la soluzione poco pratica.

2.3.2.10 Cve2att&ck: Bert-based mapping of CVEs to mitre ATT&CK techniques

In questo studio [33] si affronta un database di conoscenze sulla sicurezza informatica standardizzato annotando un dataset di CVE con tecniche MITRE ATT&CK. Lo studio in questione presenta modelli per collegare automaticamente le CVE alle tecniche utilizzando la descrizione testuale dai metadati CVE. Vengono utilizzati modelli di machine learning classici e modelli di linguaggio basati su BERT, tuttavia vengono usati set di addestramento sbilanciati e solo 1813 CVE e 31 tecniche MITRE, il miglior modello infatti ha ottenuto un F1-score[16] del 47,84%, indicando una mancanza di generalizzazione in fase di addestramento.

2.3.2.11 Linking common vulnerabilities and exposures to the mitre att&ck framework: A self-distillation approach

Un ultimo lavoro [34] mira a costruire una base di conoscenze sulla sicurezza informatica per la difesa delle infrastrutture critiche.

[16] Uno score che mette in relaziona la precision (precisione) e il recall (richiamo), se l'F1-score è basso uno dei due parametri è basso, se l'F1-score è alto i parametri sono entrambi alti.

Viene proposto il modello CVE Transformer (**CVET**) per etichettare le CVE con 10 tecniche del framework ATT&CK. Il modello utilizza il fine-tuning e la distillazione della conoscenza con RoBERTa, raggiungendo un F1-score del 76,1% nell'etichettare le CVE. Lo studio utilizza un dataset CVE da BRON [31] che fornisce classificazioni in astrazioni di alto livello, comprese le tecniche e tattiche MITRE ATT&CK. Tuttavia, il modello di cui si parla in questo studio non sembra essere di pubblico dominio, anche se lo fosse la sua percentuale di accuratezza circa sull'80% non viene considerata abbastanza sufficiente per il raggiungimento dell'obiettivo presentato, non tenendo conto comunque che non è sufficientemente addestrato per effettuare predizioni sul dominio della matrice ATLAS o sulle descrizioni delle CWE.

2.3.2.12 Conclusione

Tra tutti gli studi precedentemente riportati, i **principali problemi** che limitano l'utilizzo di ciascun modello di mappatura tra vulnerabilità e TTPs sono i seguenti:

- **nessuno** riesce a offrire una mappatura **sufficientemente precisa** tra CVE/CWE e TTPs del contesto di ATT&CK;
- **neanche uno** tra i recenti studi tratta della **matrice ATLAS**;
- gli studi che trattano anche CWE sono **troppo generali** e non si rifanno in maniera precisa a TTPs dei framworks MITRE.

Questo crea una lacuna significativa nella capacità di correlare accuratamente le vulnerabilità con le tecniche di attacco specifiche,

limitando così l'efficacia delle difese informatiche che si basano su queste correlazioni.

Nella fase di design e sviluppo di questo progetto si intraprenderà una nuova soluzione per superare queste limitazioni. L'obiettivo è usare dei metodi o tecniche che possano mappare in modo preciso le CVE e le CWE alle relative tecniche di attacco MITRE.

2.4 Analisi di un reale attacco utilizzando il framework 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 il pubblico, piccole e medie imprese e conglomerati industriali.

L'effetto immediato di tale attacco 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 questa 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 possibile creare una mappatura tra le TTPs del framework MITRE ATT&CK e l'attacco precedentemente descritto.

2.4.1 Reconaissance

Tutto è iniziato nel 2021, Fortinet ha rilevato un attacco sulla VPN "*Fortigate*" riguardante la vulnerabilità **CVE-2018-13379**

pubblicata 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

2.4.2 Initial Access

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

2.4.3 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

2.4.4 Lateral movement

Dopo aver ottenuto l'accesso iniziale attraverso le VPN non aggiornate, l'aggressore ha eseguito un lateral movment all'interno

della rete di gestione fiduciaria dirigendosi verso un segmento di rete specificamente designato per il controllo e la gestione della rete. Attraverso questo accesso avanzato, o privilage escalation, l'aggressore è stato in grado di oltrepassare la Demilitarized Zone (DMZ) e infiltrarsi nella rete intranet satellitare, 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

2.4.5 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. 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

2.4.6 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

2.4.7 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

2.4.8 Impact

In questa fase vengono presentate le ultime tecniche utilizzate per ottenere gli 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

2.5 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.

2.5.1 Q2 2022 vs Q2 2023

Un'**indagine comparativa** recente [4], che confronta i dati relativi agli attacchi informatici noti fino al Q2[17] 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.

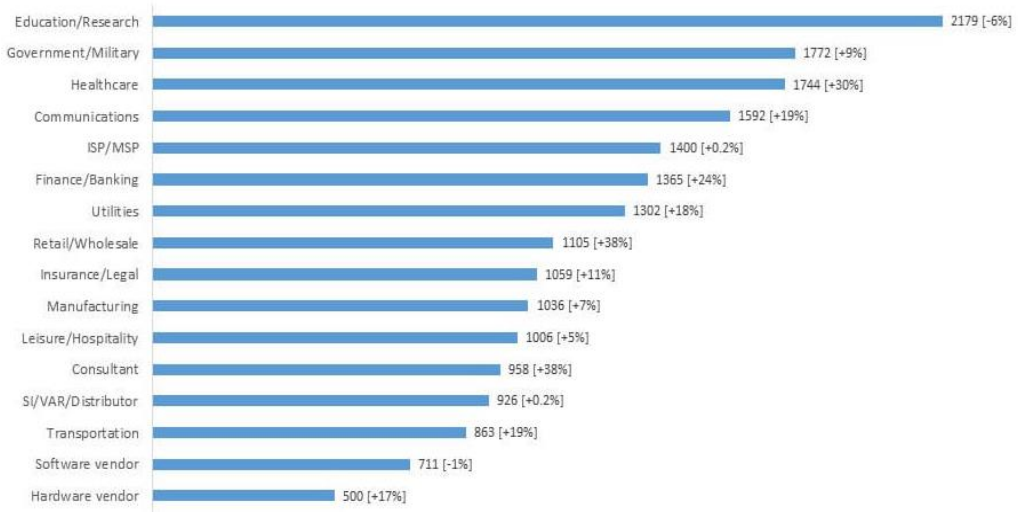

Figura 6: Q2 2022 vs Q2 2023

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**

[17] Secondo semestre

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 e prevenzione avanzate per salvaguardare dati di vitale importanza.

2.5.2 Provenienza delle cyber minacce

Un altro grande 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 la 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.

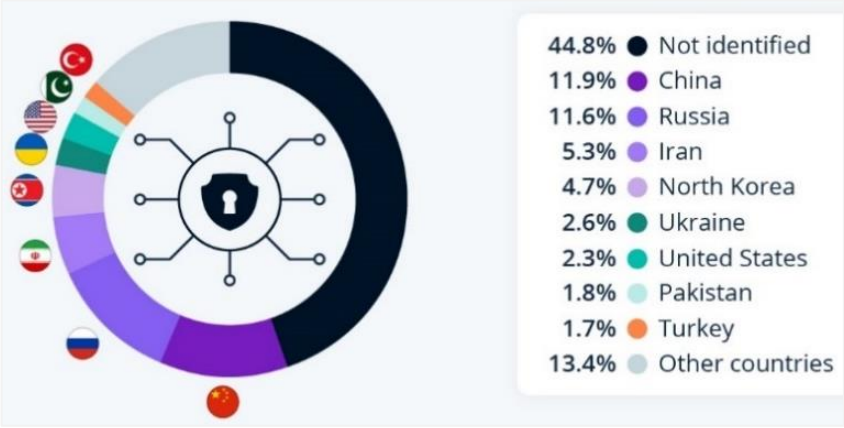

Figura 7: Provenienza dei cyber attacchi

2.5.3 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).

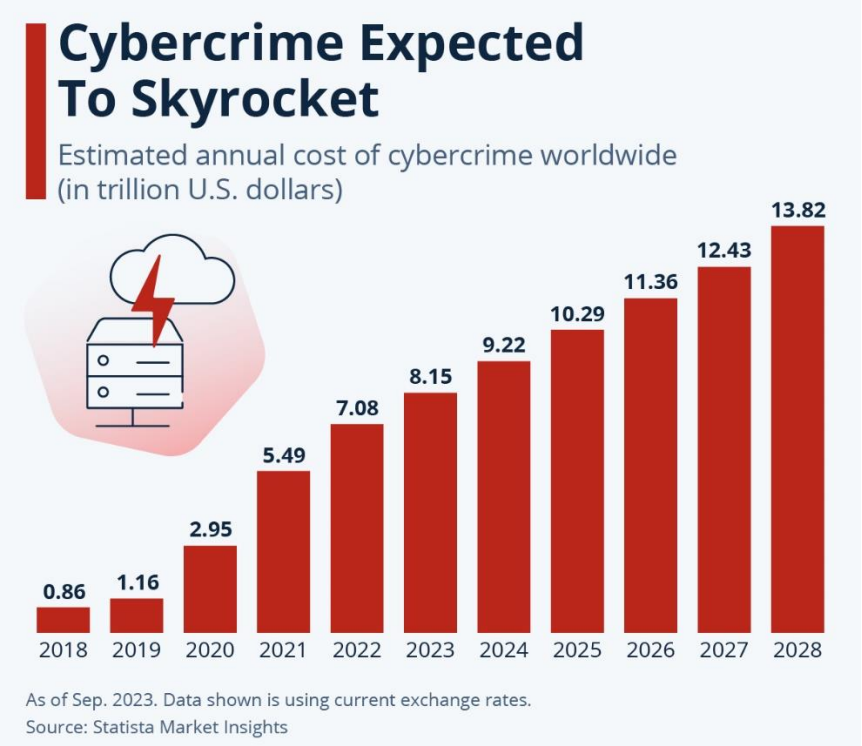

Figura 8: Stima della crescita del costo annuale per il cyber crimine

2.6 NIS2 – L'ultima normativa nel mondo cyber

Il mondo ha iniziato a mobilitarsi per rispondere alle minacce derivanti dalla evolutiva sfera informatica, molte 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. Essa 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*[18] o *autorità nazionale* entro 24 ore dall'evento.

[18] **Computer Security Incident Response Team**, gruppo di sicurezza governativo con il compito di regolamentare le cooperazioni con il settore privato nella sfera della cybersicurezza.

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, come detto precedentemente, è lo sviluppo di un sistema avanzato progettato per offrire un supporto essenziale ai professionisti del settore della sicurezza informatica, tramite una **analisi quantitativa del rischio**, denominato **DetectiveAttacks**[19].

3.1 Funzionalità di DetectiveAttacks

Il sistema proposto mira a semplificare il processo di mitigazione degli attacchi informatici diretti verso le infrastrutture digitali, attraverso l'impiego di strumenti per:

- **visualizzare** tutte le **informazioni** provenienti dalla **CTI community**, tramite un unico punto di accesso, unica interfaccia e mostrando tutte le relazioni che vi sono tra essi;

[19] https://github.com/nicolabalzano/DetectiveAttacks

- offrire il risultato dell'**unione** della matrice **ATT&CK** e **ATLAS** riordinata secondo la CKC[20];
- **classificare** le **vulnerabilità** (CVEs e CWEs) in base alle **TTPs** note e riportare nei framework utilizzati, tramite ricerca manuale o inserimento di un CTI report che le fornisca;
- studiare le **conseguenti tecniche** che potrebbero essere state **impiegate** o che **potrebbero manifestarsi** in futuro sulla successione cronologica della **CKC**, in modo da assicurare e prevenire la sicurezza nella propria organizzazione;
- offrire la **reportistica** necessaria per condurre un'analisi più approfondita del rischio associato ai vari **gruppi** e **agenti di minaccia** noti, basandosi sulle TTPs precedentemente identificate.

3.2 Tecnologie utilizzate

Durante la **fase iniziale** dello sviluppo è stato intrapreso il processo di 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,

[20] Cyber Kill Chain

prediligendo maggiormente una **metodologia** di sviluppo **orientata agli oggetti** anziché funzionale.

3.2.1 Framework, librerie e LLM utilizzati

I framework utilizzati durante lo sviluppo dell'applicativo 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).

Al contempo le API utilizzate nella produzione del sistema sono:

- **GPT-4o API from Azure**: Microsoft Azure[21] mette a disposizione le API di OpenAI per interrogare determinate versioni di modelli di

[21] Piattaforma cloud che mette a disposizione servizi di cloud computing

deep learning basati su GPT di cui è possibile effettuare il deploy tramite la medesima piattaforma.

- **cvwelib**: libreria pyhton [35] che fornisce, replica ed estende le API del NIST per ottenere le informazioni relative alle CVEs e aggiunge API per ottenere informazioni sulle CWEs.
- **capeclib**: creata durante lo sviluppo del medesimo sistema, fornisce le API per il ritrovamento delle informazioni relative ai CAPECs tramite il proprio identificativo.

3.2.2 Tipo di dati manipolato – STIX Object e dict

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 MAPPINGS EXPLORER. Gli oggetti forniti dal framework ATT&CK sono degli oggetti **STIX** (Structured Threat Information eXpression), i quali 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 e TTPs, 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 MAPPINGS 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 CVEs, CWEs e CAPECs come dizionari a causa del loro grande volume.

3.3 Architettura

L'architettura scelta per lo sviluppo dell'applicativo DetectiveAttacks è un'architettura a **microservizi** (figura 9). Questa scelta è stata fatta per diversi motivi:

- **Scalabilità**: l'architettura a microservizi consente di scalare individualmente i singoli componenti dell'applicazione in base alle esigenze. Questo significa che se una parte specifica dell'applicativo necessita di maggiori risorse, può essere scalata senza dover modificare o ridistribuire l'intera applicazione.
- **Manutenibilità**: ogni microservizio è indipendente e isolato, il che rende il codice più gestibile e più facile da mantenere.
- **Flessibilità tecnologica**: i microservizi possono essere sviluppati utilizzando tecnologie diverse, a seconda delle necessità di ciascun servizio. Questo permette di utilizzare gli strumenti e i linguaggi di programmazione più adatti per ogni specifico compito.

- **Risoluzione dei problemi**: l'isolamento dei microservizi facilita l'individuazione e la risoluzione dei problemi. Se un microservizio ha un problema, è possibile intervenire direttamente su di esso senza impattare sugli altri componenti dell'applicazione.
- **Resilienza**: i microservizi possono essere progettati per essere più resilienti, in quanto l'isolamento dei servizi riduce il rischio che un guasto in un componente comprometta l'intera applicazione. In caso di errore in un microservizio, gli altri possono continuare a funzionare normalmente, anche se in certi casi con funzionalità limitate, a meno di duplicazione di essi.
- **Macchine indipendenti**: questo tipo di architettura permette anche di creare un'applicazione dove le varie parti di essa possano essere anche su macchine differenti.

Questi vantaggi rendono l'architettura a microservizi una scelta ideale per lo sviluppo di applicazioni complesse e che manipolano dati continuamente aggiornati, come DetectiveAttacks, garantendo una maggiore efficienza, flessibilità e robustezza in casi in cui vengano inserite nuove sorgenti di dati della CTI o nuovi framework possibilmente utili che estendano le funzionalità del sistema.

L'architettura descritta verrà implementata tramite l'utilizzo di **container**[22] e della piattaforma **Docker**[23].

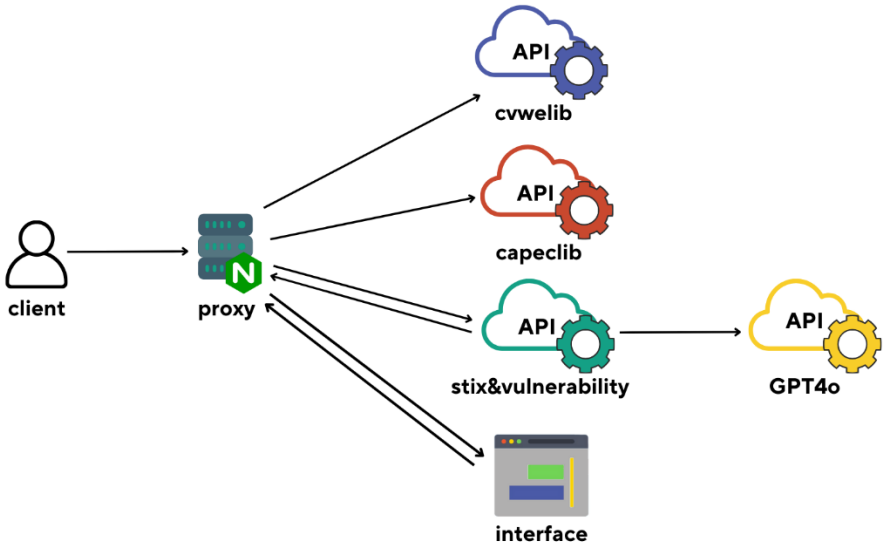

Figura 9: Architettura del software

3.3.1 Componenti dell'architettura

Le componenti presenti nel sistema attualmente sono 5:

- **nginx:** un web server utilizzato nel sistema come reverse proxy al fine di ridirezionare tutto il traffico generato, mettendo a disposizione tutte le componenti tramite un'unica porta.

---

[22] Componenti che virtualizzano un sistema operativo in modo che l'applicazione possa essere eseguita in modo indipendente su qualsiasi piattaforma. A differenza delle macchine fisiche, non virtualizzano l'intera struttura hardware.

[23] Software progettato per eseguire processi informatici in ambienti isolati e facilmente distribuibili.

- **stix&vulnerability:** fornisce e manipola i dati relativi agli STIX objects e le loro relazioni conosciute con le Vulnerabilità, in questo container vi è anche l'interfaccia che gestisce l'accesso alle API di **GPT4o**. tuttavia, quest'ultima non verrà implementata come un server Flask collegato al proxy server Nginx, poiché le tecnologie che permettono di mettere in comunicazione una componente con un server Python sono limitate dal massimo di 2048 caratteri per l'URL. Al contrario, GPT accetta fino a 50000 token[24] per i limiti concessi e utilizzati nel seguente studio, quindi nel passaggio di parametri al server si potrebbe superare il limite massimo e perdere un numero di informazioni molto importante.
- **cvwelib:** container che ospita la libreria che permette di cercare ed ottenere le informazioni sulle CVEs, CWEs e relazioni tra loro, in base a chiavi di ricerca.
- **capeclib:** container che permette di ottenere le informazioni riguardanti i CAPECs e relazioni con CVEs, CWEs e tecniche MITRE.
- **webInterface**: è il container si occupa di fornire l'interfaccia web dell'applicazione, sviluppato in **react js** con l'ausilio dei framework **bootstrap**, **react-bootstrap** e **MUI Core**.

[24] Un token corrisponde all'incirca a 4 caratteri, il numero preciso dipendente dal modello uilizzato.

3.4 stix&vulnerability

Fornisce e manipola i dati relativi agli oggetti STIX e alle loro relazioni conosciute con le vulnerabilità. Questa attività include la raccolta, l'analisi, l'organizzazione di informazioni dettagliate sugli oggetti STIX e ricerca, creazione e salvataggio di relazioni tra le Vulnerabilità con le relative TTPs.

Il microservizio in questione è interamente sviluppato in Python e mette a disposizione 2 moduli principali:

- **dataProvider**: che definisce le classi, i dati che verranno utilizzati, i metodi di elaborazione e quelli per il recupero delle informazioni dalla macchina;
- **dataAccesAPI**: che definisce il formato di condivisione dei dati ottenibili dal server Flask.

3.4.1 Data Provider

Di seguito viene illustrato il funzionamento del modulo **dataProvider** (figura 10), il quale ha il compito di definire e gestire i dati relativi ai **threats** e **relazione con le vulnerabilità**.

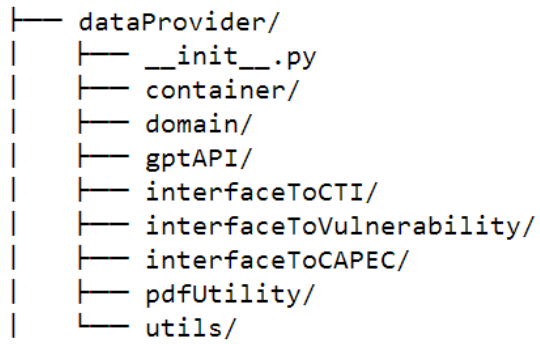

Figura 10: Struttura package

/stix&vulnerability/src/dataProvider

3.4.1.1 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 11).

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 d'istanziare nuovamente la classe comporterà il recupero dell'istanza esistente dal dizionario, anziché la creazione di una nuova istanza.

```python
def singleton(cls):
    instances = {}

    nicolabalzano
    def get_instance(*args, **kwargs):
        if cls not in instances:
            instances[cls] = cls(*args, **kwargs)
        return instances[cls]

    return get_instance
```

Figura 11: Implementazione del pattern Singleton

3.4.1.2 Interfaccia per CTI data

Per incapsulare efficacemente le funzionalità fornite dalle librerie sviluppate da MITRE e gestire la provenienza dei dati della CTI, è stato creato un package dedicato (figura 12), 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**.

```
├── interfaceToCTI/
|   ├── __init__.py
|   ├── CTIdata.py
|   ├── FetchData.py
|   ├── files/
|   ├── mappingExplorerData/
|   ├── mitreAtlasData/
|   ├── stixData/
|   └── utils/
```

Figura 12: Struttura package

/stix&vulnerability/src/dataProvider /InterfaceToCTI

3.4.1.2.1 Files

Il package files contiene l'intero database utilizzato per ottenere gli STIX objects e le relazioni di questi con le vulnerabilità (figura 13). Questo database è fondamentale per il funzionamento del sistema poiché include tutte le informazioni necessarie per correlare gli oggetti STIX con le varie minacce e vulnerabilità.

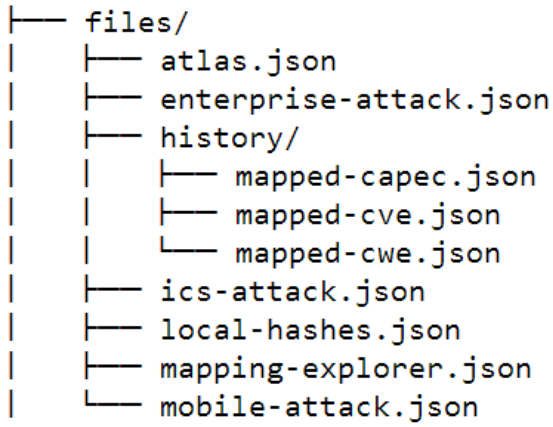

Figura 13: File per salvare ed ottenere i dati

/stix&vulnerability/src/dataProvider /InterfaceToCTI/files

3.4.1.2.2 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.json*, 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.

3.4.1.2.3 Mitre Atlas Data

Il package *mitreAtlasData* (figura 14) 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.

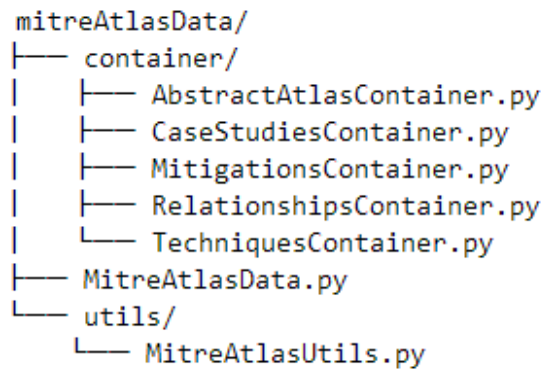

Figura 14: Struttura package

/stix&vulnerability/src/dataProvider/interfaceToCTI/mitreAtlasDat

a

3.4.1.2.4 MAPPINGS EXPLORER Data

La classe nel package *mappingsExplorerData* permette di recuperare le informazioni fornite dal framework MAPPINGS EXPLORER, incapsulando il suo funzionamento in un unico modulo, al fine di integrare questa funzionalità con le altre per riuscire ad ottenere la relazione diretta tra CVE e attack patterns MITRE.

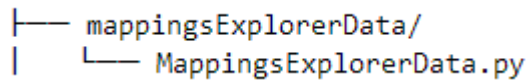

Figura 14: Struttura del package

/stix&vulnerability/src/dataProvider/InterfaceToCTI/mappingsExpl

orerData

3.4.1.2.5 STIX data

È un insieme di moduli (figura 17) che richiamano le interfacce di comunicazione con i framework ATT&CK e ATLAS, 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 struttura più diretta e accessibile dei dati contribuisce a ridurre gli errori e a facilitare le future estensioni e modifiche del codice.

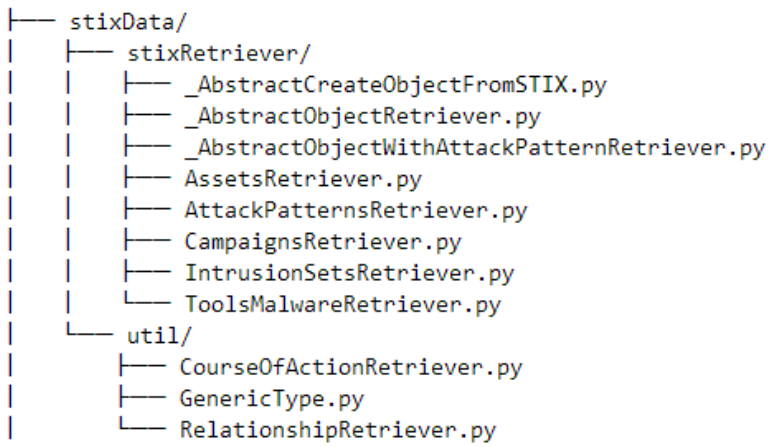

Figura 17: Struttura del package

*/stix&vulnerability/src/dataProvider/InterfaceToCTI/*stixData

3.4.1.2.5.1 STIX retriever

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**[25], **Campaign**[26], **CourseOfAction**[27], **Tool**[28], **Malware**[29], **Asset**[30] (i precedenti due oggetti non vengono distinti nei framework MITRE e prendono il nome di **Software**) e **IntrusionSet**[31], senza dover effettuare molteplici ricerche per ottenere la relazione tra essi.

3.4.1.2.6 CTI Data

Si tratta di un componente del software che svolge il ruolo di **interfaccia** ai "**dati raw**" (figura 16) provenienti dai file JSON. 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 di ATT&CK Enterprise da file JSON.
- **MITRE_ATTACK_MOBILE_DATA**: fornisce l'accesso ai dati di ATT&CK per il contesto mobile.

---

[25] Oggetto STIX che identifica una tecnica

[26] Oggetto STIX che identifica le campagne

[27] Oggetto STIX che identifica le mitigazioni

[28] Oggetto STIX che identifica i tool

[29] Oggetto STIX che identifica i malware

[30] Oggetto STIX che identifica gli asset industriali

[31] Oggetto STIX che identifica i threat group e threat agent

- **MITRE_ATTACK_ICS_DATA**: rende disponibili i dati di 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.
- **MAPPINGS_EXPLORER_DATA**: rende disponibili le relazioni tra CVEs e attack patterns del framework MAPPINGS EXPLORER.

```
MITRE_ATTACK_ENTERPRISE_DATA = MitreAttackData(default_path + ENTERPRISE_ATTACK + '.json')
MITRE_ATTACK_MOBILE_DATA = MitreAttackData(default_path + MOBILE_ATTACK + '.json')
MITRE_ATTACK_ICS_DATA = MitreAttackData(default_path + ICS_ATTACK + '.json')
MITRE_ATLAS_DATA = MitreAtlasData(default_path + ATLAS + '.json')
MAPPINGS_EXPLORER_DATA = MappingsExplorerData()
```

Figura 16: Contenuto del modulo

/stix&vulnerability/src/dataProvider/InterfaceToCTI/CTIdata

3.4.1.3 Domain

Il modulo domain del package dataProvider nel container stix&vulnerability 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, IntrusionSet e CourseOfAction, secondo quanto delineato dai vari framework MITRE, mantenendo le correlazioni tra gli oggetti.

3.4.1.3.1 MySTIXObject

Il modulo include una ridefinizione degli oggetti STIX (figura 18) per preservare, durante l'esecuzione, le relazioni tra AttackPattern

e CourseOfAction e le associazioni tra Campaign, Tool, Malware, Asset i relativi AttackPattern di riferimento.

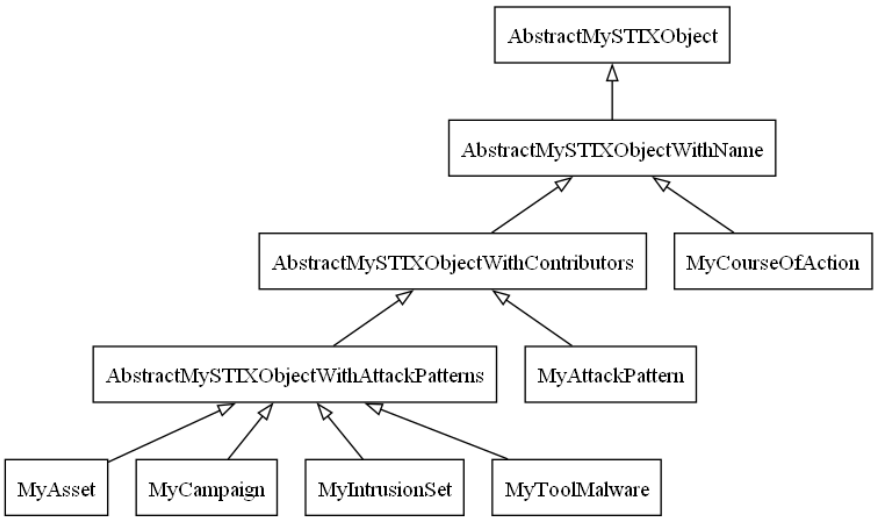

Figura 18: Ereditarietà delle classi MySTIX

3.4.1.3.1.1 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. Quest'ultime 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. Questi sono aspetti fondamentali in contesti dove il volume di dati è elevato e le performance sono critiche.

3.4.1.3.2 Attack Phase

Si tratta di un'enumerazione progettata per amalgamare e stabilire la 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 sulla Cyber Kill Chain. Attraverso l'analisi dell'ordine in cui le tattiche si manifestano nei suddetti framework, è stata ricreata la CKC, riflettendo così una strutturazione meticolosa delle fasi dell'attacco in relazione alle metodologie cyber.

Di seguito è riportata la successione cronologia delle tattiche riportate nei 2 framework riorganizzate secondo la CKC:

1. **Reconnaissance**:
    a. Reconnaissance (Enterprise, Atlas)
2. **Weaponization**:
    a. Resource Development (Enterprise, Atlas)
3. **Delivery**:
    a. Initial Access (Enterprise, Mobile, ICS, Atlas)
    b. ML Model Access (Atlas)
4. **Exploitation**:
    a. Execution (Enterprise, Mobile, ICS, Atlas)
5. **Installation**:
    a. Persistence (Enterprise, Mobile, ICS, Atlas)
    b. Privilege Escalation (Enterprise, Mobile, ICS, Atlas)

c. Defense Evasion (Enterprise, Mobile, Atlas)

d. Evasion (ICS)

6. **Command & Control**:

   a. Credential Access (Enterprise, Mobile, Atlas)

   b. Discovery (Enterprise, Mobile, ICS, Atlas)

   c. Lateral Movement (Enterprise, Mobile, ICS)

   d. Command and Control (Enterprise, Mobile, ICS)

   e. Collection (Enterprise, Mobile, ICS, Atlas)

   f. Inhibit Response Function (ICS)

7. **Action on Objectives**:

   a. Impair Process Control (ICS)

   b. ML Attack Staging (Atlas)

   c. Exfiltration (Enterprise, Mobile, Atlas)

   d. Impact (Enterprise, Mobile, ICS, Atlas)

3.4.1.4 Container

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

3.4.1.4.1 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 19). 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 presenti nei framework ATT&CK e ATLAS, basato sui loro identificativi unici o non unici sia esso un STIX ID, un MITRE ID o semplicemente il nome. 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 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 potenzialmente futuri e passati permette di adottare un approccio proattivo nella difesa, anticipando le mosse degli avversari, e al contempo permette 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.

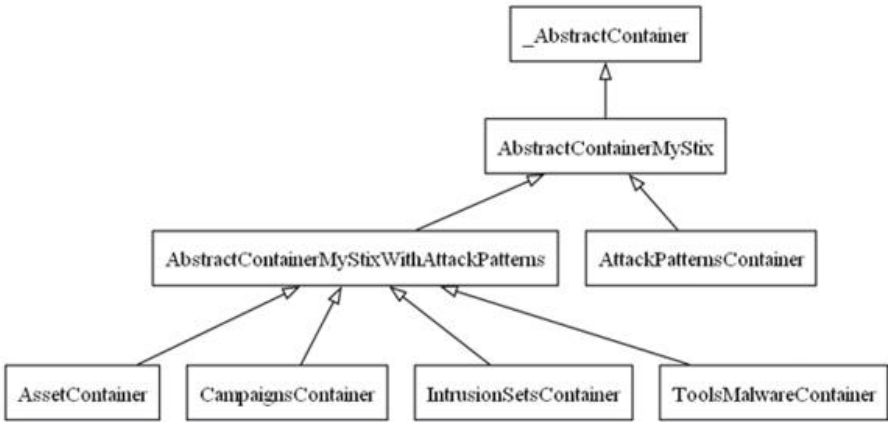

Figura 19: Ereditarietà delle classi container

3.4.1.4.2 Mitre to Vulnerability Container

Questo package (figura 20) contiene la classe **MitreToVulnerabiltyContainer**, la quale ha il compito di recuperare il mapping tra la vulnerabilità e i MITRE attack patterns.

Per ottenere la relazione in questione viene seguito un approccio condizionale complesso (figura 21).

Nel caso in cui la vulnerabilità cercata sia una **CWE**:

- viene verificata la presenza della mappatura all'interno del file *mapped-cwe.json* (figura 13), in cui vengono salvate le relazioni precedentemente cercate al fine di minimizzare il tempo di risposta del sistema.
- Se il mapping è presente nel file che contiene le history allora viene **restituita la relazione**,
- altrimenti si cercano i **CAPEC ids** relativi alla CWE:
    - Se **esistono CAPEC ids** relativi alla CWE viene cercata la **relazione** tra questi e gli attack patterns del **framework ATT&CK** all'interno del file *mapped-capec.json* (figura 13) e la libreria capeclib e restituita se trovata.
    - Se **esistono i CAPEC ids** ma **nessuno** di essi ha una **relazione** con gli attack patterns MITRE, viene effettua una **query ad un LLM**, per ogni CAPEC al fine di creare il mapping e salvarlo in *mapped-capec.json* (figura 13).
    - Se **non vi sono CAPEC ids** relativi alla vulnerabilità allora viene effettuata una **richiesta ad un LLM** al fine di ottenere la

relazione tra la CWE e gli attack patterns MITRE, successivamente salvata nel file *mapped-cwe.json* (figura 13).

Nel caso in cui la vulnerabilità cercata sia una **CVE**:

- Viene verificata la presenza della mappatura all'interno del file ***mapped-cve.json*** (figura 13), in cui vengono salvate le relazioni precedentemente cercate, relative alle CVE, al fine di minimizzare il tempo di risposta del sistema.
- Se la relazione è presente viene **restituita** immediatamente,
- altrimenti se **non è presente**, viene effettuata la ricerca della CVE all'interno del framework **MAPPINGS EXPLORER**.
    - Qualora la relazione sia **presente** all'interno del framework, viene salvata nel file *mapped-cve.json* (figura 13), diminuendo i tempi di risposta per la medesima ricerca e successivamente **restituita**,
    - altrimenti vengono **cercate** le **CWEs** relative alla CVE.
        - Se quest'ultima relazione è presente viene ripreso il **percorso** di mapping di una CWE **precedentemente** descritto, salvando la nuova relazione in *mapped-cve.json* (figura 13).
    - Tuttavia **se non vi sono CWEs** relative alla CVE, viene effettuata una **richiesta ad un LLM**, ottenendo gli attack patterns MITRE relativi alla vulnerabilità in questione,

salvando il mapping in *mapped-cve.json* (figura 13) e successivamente restituito.

Riassumendo, viene effettuata prima la ricerca negli appositi file di history (figura 13), qualora la relazione non fosse presente vengono verificate le relazioni tra le vulnerabilità e TTPs precedentemente mappate dalla CTI, salvate e restituite. Inoltre ad ogni nuovo mapping riscontrato il sistema memorizza negli appositi file JSON sia le singole relazioni, che servono ad ottenere la relazione finale con la vulnerabilità, come nel caso dei CAPECs, sia la stessa relazione iniziale cercata.

Le relazioni tra CVE/CWE/CAPEC con le TTPs di ATT&CK e ATLAS vengono salvate seguendo lo stesso approccio del framework MAPPINGS EXPLORER ma inserendo le tecniche sempre nella classe "*uncategorized"* (nel caso di CVE o CWE) e salvando la fonte da cui proviene la relazione ottenuta (figura 22).

Le possibili fonti dipendono da come viene ottenuta la relazione e sono:

- **MAPPINGS_EXPLORER**, se provengono dal medesimo framework;
- **CAPEC**, se sono ottenute tramite la relazione tra CWE e CAPEC id;
- **REQUEST_CAPEC**, qualora la relazione sia ottenuta tramite la richiesta ad un LLM delle TTPs relative ad un CAPEC;
- **REQUEST_CWE**, qualora la relazione sia ottenuta tramite la richiesta ad un LLM delle TTPs relative ad una CWE;

- **REQUEST_CVE**, qualora la relazione sia ottenuta tramite la richiesta ad un LLM delle TTPs relative ad una CVE.

```
├── mitreToVulnerabilityContainer/
│   └── MitreToVulnerabilityContainer.py
```

Figura 20: Struttura del package */stix&vulnerability/src/dataProvider/container/mitreToVulnerabilityContainer*

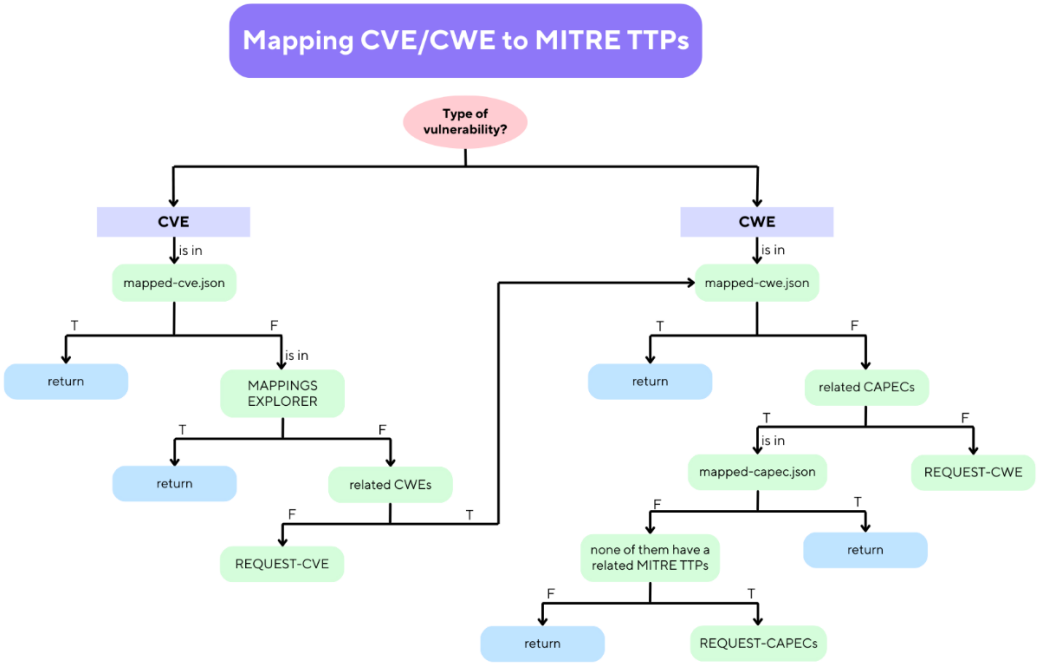

Figura 21: Approccio condizionale per il recupero della relazione tra vulnerabilità e MITRE TTPs

```
"CWE-62": {
    "exploitation_techniques": [],
    "primary_impact": [],
    "secondary_impact": [],
    "uncategorized_impact": [
        "T1122",
        "T1072"
    ],
    "relationship_source": " REQUEST-CWE"
}
```


Figura 22: Esempio di salvataggio del mapping ottenuto tramite una richiesta al modello scelto

3.4.1.4.2.1 Prima strada intrapresa – Modelli preaddestrati

La prima strada intrapresa è stata quella di testare come LLM potenzialmente utilizzabili i modelli di machine learning descritti a stato dell'arte.

Tuttavia, come precedentemente spiegato, le loro limitazioni non permettono il medesimo utilizzo nello sviluppo di questo applicativo. Infatti in fase di testing, ad una singola vulnerabilità venivano correlate un numero troppo elevato di tecniche MITRE, confermando gli svantaggi presentati.

Il problema principale nell'utilizzo di questi LLM è che sono addestrati su dataset ridotti, vista la grande vastità di dati delle informazioni riguardanti la CTI e i termini specifici, il che li rende inutilizzabili poiché incapaci di generalizzare correttamente sui dati di apprendimento. Inoltre il framework ATT&CK come ATLAS sono in continua evoluzione e questo rende i modelli in quesitone

obsoleti già in poco tempo, senza un corretto e continuo aggiornamento.

Per ovviare a queste problematiche si è pensato di utilizzare una IA generativa in grado di elaborare e apprendere perfettamente qualsiasi tipo di testo. Questa funzionalità è cruciale, in quanto, ricevendo tramite prompt le TTPs più recenti dei framework ATT&CK e ATLAS, permette al modello di rimanere aggiornato. In questo modo si possono ottenere risposte attuali e precise e si riesce a gestire efficacemente le informazioni del dominio della CTI, superando il problema dei dati obsoleti e garantendo un'accurata interpretazione e correlazione dei dati.

3.4.1.4.2.2 Seconda strada intrapresa – Utilizzo di generative AI

La seconda soluzione, come preannunciato, prevede l'utilizzo di una IA[32] generativa, tra quelle esistenti è stata scelta **GPT4o** di OPENAI, ottenuta e distribuita tramite Microsoft Azure.

Per ottenere le relazioni tra TTPs e CVE/CWE per ogni mappatura vengono effettuate 2 richieste all'IA generativa:

1. La **prima richiesta** permette di determinare il dominio a cui la vulnerabilità si riferisce tra i seguenti: **Enterprise**, **ICS**, **Mobile** e **Artifical Intelligence**, in modo da definire quali sono le TTPs su cui il

[32] Intelligenza Artificiale

modello dovrà ragionare per prendere la decisione successivamente richiesta.

2. La **seconda richiesta** utilizza la risposta ottenuta dal primo prompt per definire quale query effettuare. In base al dominio ottenuto precedentemente, viene fornito al modello un prompt che, tramite il ruolo di "system", include tutte le tecniche parent[33] conosciute per quel dominio, ognuno con il proprio ID, nome e primo paragrafo della descrizione in modo da fornire al modello le conoscenze necessarie per cercare la relazione. Contestualmente, come "user", viene fornita la descrizione della vulnerabilità, chiedendo al modello di restituire, in un formato JSON, la lista dei MITRE ID degli attack-patterns correlati.

Utilizzando quindi questi prompts, dalla dimensione totale di circa 18000 token, è possibile generare una nuova mappatura, la quale verrà successivamente salvata nell'apposito file JSON in base all'approccio precedentemente descritto. Di conseguenza, le ricerche future della stessa vulnerabilità risulteranno meno computazionalmente onerose, grazie alla disponibilità immediata della correlazione precedentemente determinata.

[33] Cioè le tecniche aventi ID nel formato T0000 o AML.T0000, dove gli 0 sono dei numeri identificativi

3.4.1.5 gptAPI

Per ottenere una nuova relazione, come precedentemente descritto, viene utilizzato il modulo **gptAPI**. Il presente modulo consente di comunicare con il modello distribuito tramite Microsoft Azure, attraverso la classe **GPT_API**, la quale fornisce le funzioni per effettuare richiesta delle due query descritte in precedenza.

3.4.1.6 PDF Utility

Nel container stix&vulnerability vi è anche un modulo che incapsula la manipolazione dei file in formato PDF. In questo modulo vi sono 2 sotto moduli.

3.4.1.6.1 PDF Generation

Pdf Generation incapsula il comportamento della libreria **pdfkit**, la quale, tramite l'utilizzo del package **wkhtmltopdf**, permette di generare un file in formato .pdf partendo dal formato HTML. Questa funzionalità viene utilizzata per andare a generare un report che dato un insieme di attack-patterns riscontrati, fornisce la probabilità con cui si sta subendo un attacco informatico da parte degli Instrusion Set conosciuti.

3.4.1.6.2 PDF Extraction

PDF Extraction integra il comportamento della libreria **pypdf**. La libreria in questione viene utilizzata per andare a estrarre il testo da un file in formato PDF. Questa funzionalità permette di andare

ad implementare la funzione di lettura di un CTI report ed estrazione delle vulnerabilità in esso presenti.

3.4.1.7 Interfaccia per cvwelib

All'interno di stix&vulnerability è presente anche un modulo che ha il compito di fornire un'interfaccia per effettuare le query ed ottenere le vulnerabilità dal container che distribuisce la libreria cvwelib (figura 23), tramite i moduli **CVE.py** e **CWE.py**. Questo approccio offre diversi vantaggi significativi. In primo luogo, centralizzando l'accesso alle informazioni sulle vulnerabilità, si semplifica notevolmente il processo di recupero dei dati, rendendo più efficiente l'interazione con il sistema. Tramite ciò è facile effettuare query specifiche senza dover comprendere la complessità interna della libreria cvwelib. In secondo luogo, questa interfaccia permette una maggiore flessibilità nell'aggiornamento e nella manutenzione del sistema. Qualsiasi cambiamento nella struttura dei dati o nelle fonti di aggiornamento può essere gestito all'interno del modulo cvwelib senza influenzare gli utenti finali o altre parti del sistema. Questo separa chiaramente le responsabilità e facilita la gestione del codice.

Un altro vantaggio è la possibilità di estendere le funzionalità del sistema. Con un modulo dedicato all'interfaccia delle query, diventa più semplice aggiungere nuove fonti di dati o implementare nuove funzionalità di ricerca e filtraggio senza dover riscrivere o modificare significativamente altre parti del sistema.

Pertanto questa organizzazione modulare migliora la scalabilità e la robustezza del sistema, consentendo di effettuare test e debug in modo più efficace.

3.4.1.8 Interfaccia per capeclib

Il modulo *interfaceToCAPEC*, ha il compito di comunicare con il continer *capeclib*, tramite **CAPEC.py**, al fine di ottenere le informazioni necessarie per effettuare il mapping tra vulnerabilità e tecniche di attacco.

I vantaggi, nell'utilizzo di un'interfaccia per contenere la comunicazione con il container esterno in questione, sono i medesimi spiegati al punto precedente per *cvwelib*.

3.4.2 Data Acces API

La struttura del package **dataAccessAPI** è organizzata per facilitare l'accesso e la manipolazione dei dati, rendendoli più leggibili e facilmente utilizzabili dagli altri componenti del sistema.

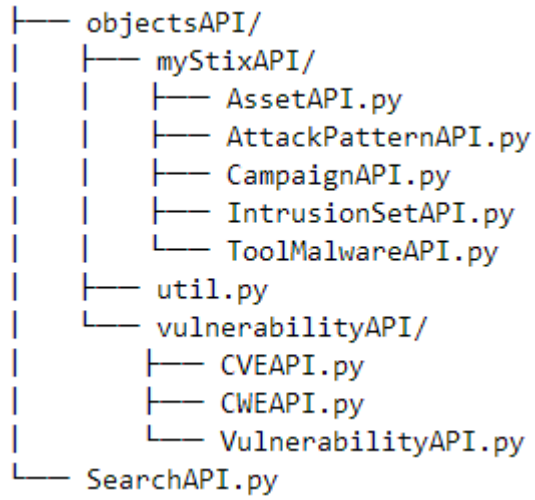

Figura 23: Struttura del package

/stix&vulnerability/src/dataAccesAPI/

3.5 cvwelib

Questo container fornisce le API per ottenere le informazioni delle vulnerabilità (CVE e CWE). Il container include un server Flask che mette a disposizione la libreria **cvwelib** [35]. La libreria in quesitone, verifica ogni giorno all'orario 00:30 la presenza di aggiornamenti dei dati riguardanti CVE e CWE (ai seguenti repository https://cwe.mitre.org/data/xml/cwec_latest.xml.zip e https://github.com/fkie-cad/nvd-json-data-feeds/releases/latest/download/CVE-Modified.json.xz), visto che dallo storico delle commit ai repository è visibile che i nuovi dati vengono caricati all'orario 00:00 di ogni giorno, facendo ciò è possibile aggiornare i dati locali secondo la nuova conoscenza della CTI community.

3.5.1 Struttura della libreria

All'interno di questa libreria (figura 24), troviamo diversi moduli che svolgono funzioni specifiche:

1. Il modulo **CWEHelper.py** nella directory cwelib/ gestisce le operazioni relative alle CWE, inclusa la verifica e il download dei dati dal repository CWE ufficiale.
2. Il modulo **NVDHelper.py** nella directory nvdlib/ si occupa delle operazioni relative alle Common Vulnerabilities and Exposures (CVE), incluso il controllo e il download dei dati dal repository NVD (National Vulnerability Database).
3. Il modulo **CWEPrettify.py** nella directory utils/ è utilizzato per convertire i dati CWE dal formato XML al formato JSON, rendendoli più leggibili e facilmente utilizzabili.
4. Infine il modulo **cvwelib.py** definisce le funzioni che svolgono il ruolo di interfaccia di accesso per effettuare le query al server Flask.

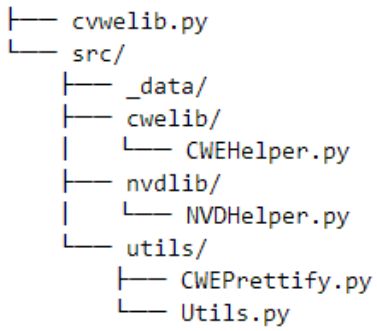

Figura 24: Struttura del package

/cvwelib

3.5.2 Vantaggio rispetto alle NIST API

Per sviluppare l'applicativo in questione è stata utilizzata questa libreria e non quella ufficiale rilasciata dal NIST [36] poiché quest'ultima pone dei limiti di richiesta quando si effettuano ripetute query in lassi di tempi minimi, inoltre non permette di ottenere le informazioni riguardanti le CWE, ma solo quelle relative alle CVE. Inoltre essendo un server locale permette dei tempi di risposta più che ridotti rispetto alle API rilasciate dal NIST.

3.6 capeclib

In questa libreria contenuta in container che prende il suo stesso nome (figura 9), ospitando il medesimo server Flask, presenta la logica di ritrovamento e aggiornamento dei dati riguardanti i CAPEC.

3.6.1 Struttura della libreria

La struttura della libreria (figura 25) è la seguente:

- **app.py**: questo file rappresenta il punto di ingresso dell'applicazione. Qui viene inizializzata e configurata l'applicazione, e vengono avviati i vari processi necessari.
- **src/**: la cartella src contiene il codice sorgente principale della libreria.
    - **_data/**: questa cartella contiene i dati utilizzati dalla libreria. In particolare, tra cui **local-**

hashes.json, che memorizza gli hash locali dei dati per determinare la necessità di aggiornamenti e **stix-capec.json**, che contiene i dati CAPEC, utilizzati per correlare e analizzare le tecniche di attacco.

- **CapecData.py**: questo file contiene la logica principale per la gestione e l'elaborazione dei dati CAPEC. Qui vengono implementate le funzioni per il caricamento, l'aggiornamento e la manipolazione dei dati relativi ai Common Attack Pattern Enumeration and Classification.
- **utils/**: questa cartella contiene vari utility scripts che supportano le funzionalità principali della libreria. Il modulo più importante in essa è **FetchData.py,** il quale si occupa del recupero dei CAPEC dalla fonte https://raw.githubusercontent.com/mitre/cti/master/capec/2.1/stix-capec.json.

Questa struttura modulare e organizzata consente di mantenere il codice pulito, facilmente manutenibile e scalabile, facilitando l'integrazione e l'aggiornamento dei dati CAPEC nel sistema.

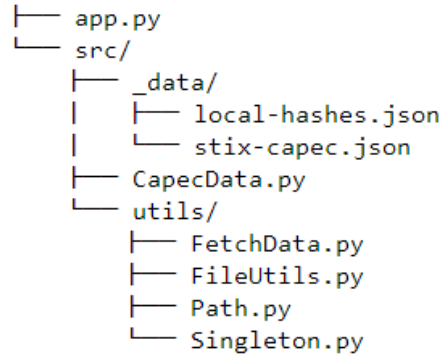

Figura 25: Struttura package

/capeclib

3.7 webInterface

L'interfaccia utente di DetectiveAttacks è stata sviluppata come applicazione web utilizzando **React.js**, un framework JavaScript noto per la costruzione di interfacce interattive e dinamiche. React.js è stato scelto per la sua capacità di gestire componenti riutilizzabili e stati complessi, permettendo la creazione di un'interfaccia moderna ed efficiente. Per ottimizzare ulteriormente il processo di sviluppo è stato impiegato **Vite**, uno strumento di build che offre un ambiente di sviluppo rapido e una configurazione semplificata. Vite facilita l'uso delle funzionalità avanzate di JavaScript moderno e migliora il workflow degli sviluppatori, riducendo i tempi di build.

La web interface si compone di differenti pagine le quali permettono di utilizzare le diverse funzionalità del sistema.

3.7.1 Searching choices

L'interfaccia di scelta della modalità di ricerca (figura 26) permette di effettuare due operazioni, avviare il sistema in ricerca manuale o caricare un report in formato PDF, CSV o TXT in modo estrarre le vulnerabilità presenti in esso. Se viene scelta la seconda opzione verranno mostrate all'utente la lista di vulnerabilità riscontrare e la possibilità di visualizzare le informazioni che il sistema ha appreso su quelle vulnerabilità.

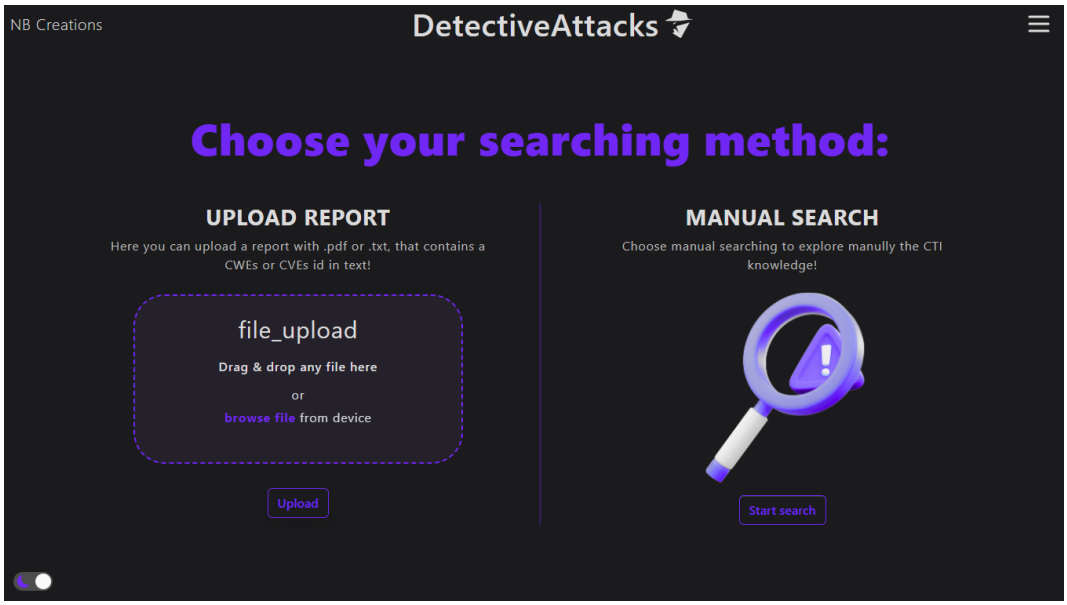

Figura 26: Searching choices page

3.7.2 Manual searching page

La pagina di ricerca manuale (figura 27) permette di esplorare l'intera knowloge base della CTI, tramite la barra di ricerca e i filtri che permettono di ottenere più agevolmente gli oggetti cercati e le relazioni con gli altri agenti di minaccia e possibili azioni difensive, gli esperti del settore possono esplorare velocemente le soluzioni

da intraprendere per la propria organizzazione o le possibili minacce per essa.

Nella stessa schermata è anche presente l'opzione per poter effettuare il mapping di una vulnerabilità, tramite il suo id, con gli attack patterns MITRE conosciuti (figura 28), in modo da conoscerne i possibili pattern di attacco sfruttati.

Figura 27: Manual searching page

Figura 28: Mapping di una nuova vulnerabilità

3.7.3 Attack patterns by phase

Nella schermata in questione si può visualizzare una matrice espansa (figura 29), la quale fornisce l'unione delle tecniche provenienti dai framework ATT&CK e ATLAS, dando così un'altra forma di visualizzazione delle informazioni e la possibilità di selezionare gli attacchi riscontrati tramite software di terze parti nella propria organizzazione al fine di generare un report (figura 30) che fornisca la probabilità con cui si sta subendo un attacco da parte dei threat agent/group conosciuti.

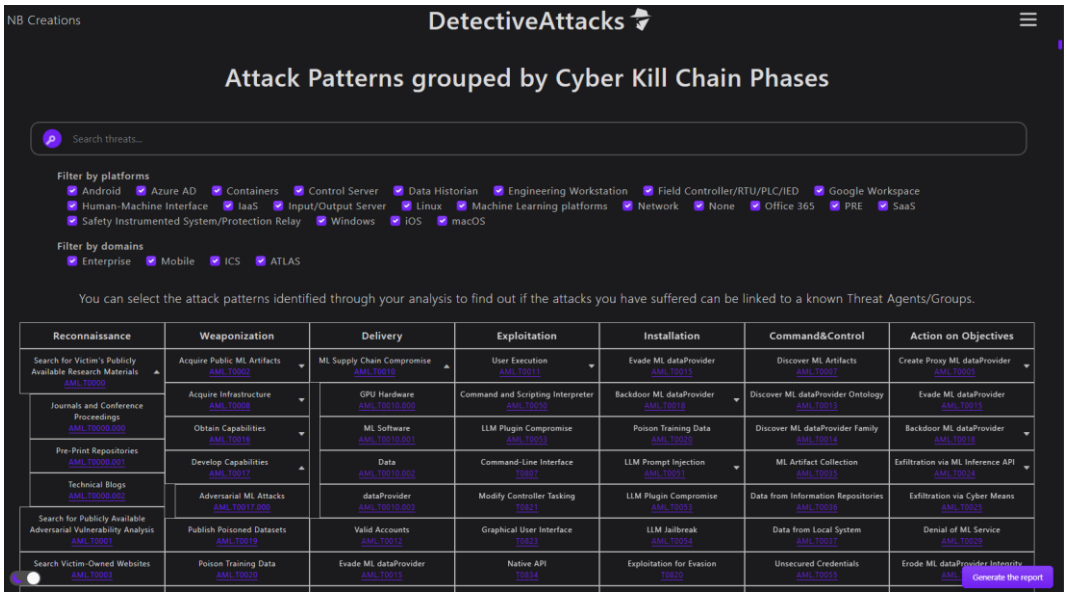

Figura 29: Unione delle matrici ATT&CK e ATLAS

Threat Agents/Groups Detected

For selected Attack Patterns

Domains (attack-pattern--40f5caa0-4cb7-4117-89fc-d421bb493df3) (T1583.001)
Email Accounts (attack-pattern--65013dd2-bc61-43e3-afb5-a14c4fa7437a) (T1585.002)
Tool (attack-pattern--a2fdce72-04b2-409a-ac10-cc1695f4fce0) (T1588.002)
Malware (attack-pattern--7807d3a4-a885-4639-a786-c1ed41484970) (T1588.001)
Spearphishing Link (attack-pattern--2b742742-28c3-4e1b-bab7-8350d6300fa7) (T1566.002)
Spearphishing Attachment (attack-pattern--2e34237d-8574-43f6-aace-ae2915de8597) (T1566.001)
Match Legitimate Name or Location (attack-pattern--1c4e5d32-1fe9-4116-9d9d-59e3925bd6a2) (T1036.005)
Pass the Hash (attack-pattern--e624264c-033a-424d-9fd7-fc9c3bbdb03e) (T1550.002)
LSASS Memory (attack-pattern--65f2d882-3f41-4d48-8a06-29af77ec9f90) (T1003.001)
Data from Local System (attack-pattern--3c4a2599-71ee-4405-ba1e-0e28414b4bc5) (T1005)
System Service Discovery (attack-pattern--322bad5a-1c49-4d23-ab79-76d641794afa) (T1007)
System Network Configuration Discovery (attack-pattern--707399d6-ab3e-4963-9315-d9d3818cd6a0) (T1016)
Remote Desktop Protocol (attack-pattern--eb062747-2193-45de-8fa2-e62549c37ddf) (T1021.001)
System Network Connections Discovery (attack-pattern--7e150503-88e7-4861-866b-ff1ac82c4475) (T1049)
Process Discovery (attack-pattern--8f4a33ec-8b1f-4b80-a2f6-642b2e479580) (T1057)
Local Account (attack-pattern--25659dd6-ea12-45c4-97e6-381e3e4b593e) (T1087.001)

APT1 (G0006): 92.54%

[APT1](https://attack.mitre.org/groups/G0006) is a Chinese threat group that has been attributed to the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398. (Citation: Mandiant APT1)

stix id: intrusion-set--6a2e693f-24e5-451a-9f88-b36a108e5662

Aliases: APT1, Comment Crew, Comment Group, Comment Panda

Domains: enterprise-attack

x_mitre_version: 1.4

Kimsuky (G0094): 4.61%

[Kimsuky](https://attack.mitre.org/groups/G0094) is a North Korea-based cyber espionage group that has been active since at least 2012. The group initially focused on targeting South Korean government entities, think tanks, and individuals identified as experts in various fields, and expanded its operations to include the United States, Russia, Europe, and the UN. [Kimsuky](https://attack.mitre.org/groups/G0094) has focused its intelligence collection activities on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.(Citation: EST Kimsuky April 2019)(Citation: BRI Kimsuky April 2019)(Citation: Cybereason Kimsuky November 2020)(Citation: Malwarebytes Kimsuky June 2021)(Citation: CISA AA20-301A Kimsuky) [Kimsuky] (https://attack.mitre.org/groups/G0094) was assessed to be responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise; other notable campaigns include Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).(Citation: Netscout Stolen Pencil Dec 2018)(Citation: EST Kimsuky SmokeScreen April 2019)(Citation: AhnLab Kimsuky Kabar Cobra Feb 2019) North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name [Lazarus Group]

1 of 3

Figura 30: Pagina di esempio del report che fornisce la probabilità di attacco da parte dei vari threat agents/groups

3.8 nginx

Nginx è stato implementato come **reverse server proxy** (figura 9) all'interno del sistema per la distribuzione delle richieste HTTP tra diversi servizi contenuti nel progetto. La configurazione di Nginx utilizzata è stata progettata per inoltrare le richieste ricevute sulla porta 80 ai rispettivi servizi in base al percorso dell'URL. Questo approccio consente una distribuzione efficiente del traffico e assicura che le richieste vengano indirizzate al servizio appropriato in modo trasparente per gli utenti del sistema.

L'integrazione di Nginx come reverse proxy server nel sistema offre la **possibilità** di implementare il **bilanciamento del carico**, il che diventa particolarmente vantaggioso se DetectiveAttacks verrà rilasciato su una piattaforma online. Con il load balancing, Nginx può distribuire le richieste tra più istanze del servizio DetectiveAttacks, garantendo una **distribuzione uniforme** del carico e migliorando le prestazioni complessive del sistema. Questo è essenziale soprattutto in ambienti online ad alto traffico, dove il load balancing aiuta a mantenere la **stabilità** e **l'affidabilità** del servizio, consentendo una maggiore scalabilità per gestire un numero crescente di utenti e richieste. Inoltre, il load balancing può fornire una maggiore **tolleranza ai guasti**, in quanto se uno dei server fallisce, le richieste possono essere indirizzate automaticamente agli altri server disponibili garantendo un'esperienza utente continua e affidabile.

3.9 Esempio di immissione di un report

Per effettuare dei test manuali del sistema e fornire un esempio pratico di utilizzo è stata eseguita un'analisi del container *stix&vulnerability* utilizzando il tool **Fortify**. Lo scopo era ottenere il report risultante da questa analisi e utilizzarlo come input per **DetectiveAttacks**.

La Static Code Analysis (**SCA**) effettuata ha evidenziato la presenza di 7 difetti all'interno del codice. Tra questi difetti, sono state identificate specificamente le seguenti CWE (figura 31):

1. Improper Input Validation (**CWE-20**),
2. Empty Exception Block (**CWE-1069**),
3. Use of Weak Hash (**CWE-328**).

Grazie al sistema sviluppato una volta conosciute queste CWE è possibile andare a studiare quali sono le tecniche che possono manifestarsi se le relative vulnerabilità non vengano eliminate.

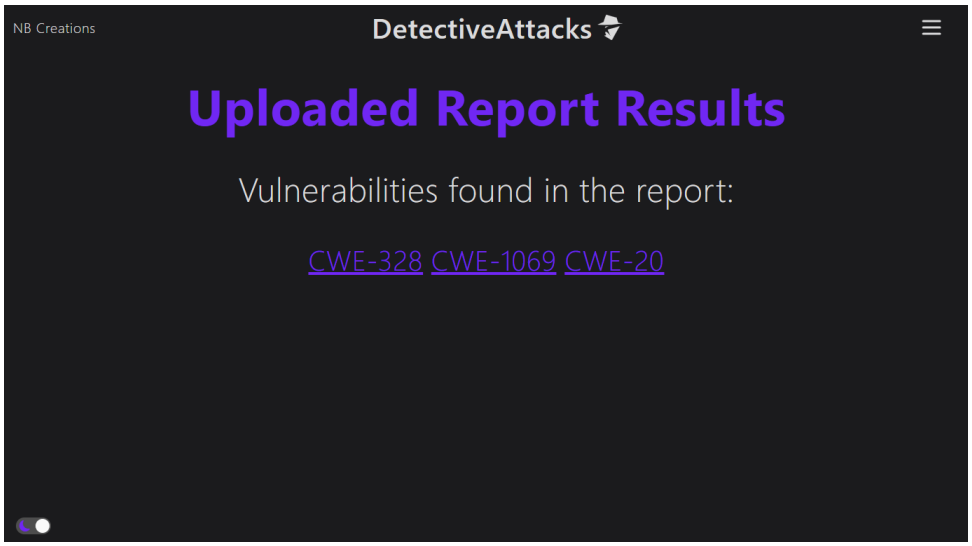

Figura 31: Vulnerabilità presenti nel SCA report

3.9.1 CWE-20

Per quanto riguarda la vulnerabilità di "Improper Input Validation", le tecniche MITRE correlate ad essa sono molteplici, evidenziando quindi la priorità nell'eliminazione di questo difetto. Tutte le tecniche di attacco possibilmente utilizzabili a seguito della CWE-20 restituite dal sistema (figura 32) sono:

- *Steal Web Session Cookie* (T1539)
- *Exploitation of Remote Services* (T1210)
- *Invalid Code Signature* (T1036.001)
- *Path Interception by PATH Environment Variable* (T1574.007)
- *Group Policy Discovery* (T1615)
- *Impair Command History Logging* (T1562.003)
- *Obfuscated Files or Information* (T1027)
- *Indirect Command Execution* (T1202)
- *Data Manipulation* (T1565)
- *Code Signing* (T1553.002)
- *Dynamic Linker Hijacking* (T1574.006)

DetectiveAttacks, come già descritto, ci fornisce anche le possibili tecniche che possono essere successivamente o precedentemente utilizzate a seguito di quelle ottenute dalla relazione (figura 33) al fine di compiere una analisi quantitativa approfondita sui rischi legati alla presenza di tale vulnerabilità.

Figura 32: Attack patterns MITRE correlati alla CWE-20

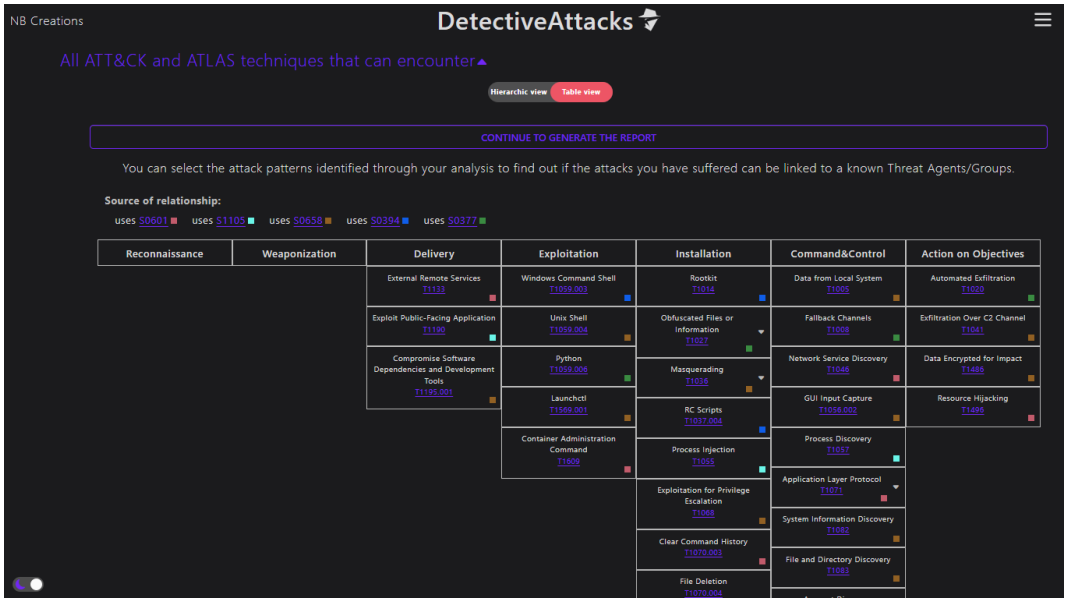

Figura 33: Parte degli attack patterns correlati a quelli sfruttati dalla CWE-20

3.9.2 CWE-1069

Riguardo la CWE-1069, conosciuta con il nome di “Empty Exception Block”, il sistema ha rilevato soltanto una tecnica di attacco

correlata a questa vulnerabilità, anche se non di poca importanza poiché si tratta di *Indirect Command Execution* (T1202).

3.9.3 CWE-328

Infine, come ultima vulnerabilità riscontrata, la CWE-328, nota come "Use of Weak Hash", il tool presenta come attack patterns MITRE correlato, la tecnica *Code Signing* (T1553.002).

3.9.4 Considerazioni

DetectiveAttacks non solo fornisce **suggerimenti per mitigare le vulnerabilità** in base alla fase di creazione del sistema (ad esempio Design, Operation o Implementation), ma offre anche altre informazioni utili.

Attraverso la conoscenza delle tecniche di attacco specifiche correlate alle vulnerabilità, il sistema consente di ottenere i **metodi di rilevamento** delle tecniche stesse, le **piattaforme** che ne vengono **colpite**, i **software** che utilizzano tali tecniche, **esempi dimostrativi** per fini benevoli e **campagne realmente avvenute** che utilizzano gli stessi patterns di attacco.

Questo approccio facilita un'analisi quantitativa completa del rischio associato a ogni vulnerabilità, permettendo di adottare misure preventive e correttive in maniera tempestiva e mirata.

3.10 Conclusioni

L'analisi effettuata con DetectiveAttacks ha dimostrato l'efficacia del sistema nel rilevare vulnerabilità specifiche e nel fornire una mappatura dettagliata delle tecniche di attacco correlate, insieme ai metodi di mitigazione. Inoltre, il sistema offre informazioni cruciali riguardanti la rilevazione, le conseguenze e gli esempi dimostrativi delle tecniche o vulnerabilità conosciute, che si dimostrano essere di fondamentale importanza.

Questo **strumento** si rivela **indispensabile** per una **gestione proattiva** delle vulnerabilità, consentendo di **anticipare potenziali attacchi** e di rafforzare la sicurezza del sistema in modo mirato. La capacità di DetectiveAttacks di aggiornare continuamente i dati e di adattarsi ai nuovi scenari di minaccia rappresenta un **valore aggiunto significativo**, garantendo una protezione costante e aggiornata contro le vulnerabilità emergenti.

Pertanto l'**obiettivo** inizialmente posto riguardante l'implementazione di soluzioni innovative per l'utilizzo di un approccio proattivo alla sicurezza informatica si considera **raggiunto**, grazie allo sviluppo di **DetectiveAttacks** e le seguenti funzionalità implementate:

- **visualizzazione** di tutte le **informazioni** provenienti dalla **CTI community**, tramite un unico punto di accesso, unica interfaccia, mostrando tutte le relazioni che vi sono tra essi;

- **unione** della matrice **ATT&CK** e **ATLAS** riordinata secondo la CKC[34];
- **classificazione** delle **vulnerabilità** (CVEs e CWEs) in base alle **TTPs** note e riportare nei framework utilizzati, tramite ricerca manuale o inserimento di un CTI report che le fornisca;
- studio delle **conseguenti tecniche** che potrebbero essere state **impiegate** o che **potrebbero manifestarsi** in futuro sulla successione cronologica della **CKC**, in modo da assicurare e prevenire la sicurezza nella propria organizzazione;
- generazione della **reportistica** necessaria per condurre un'analisi più approfondita del rischio associato ai vari **gruppi** e **agenti di minaccia** noti, basandosi sulle TTPs precedentemente identificate.

[34] Cyber Kill Chain

SVILUPPI FUTURI

Per **migliorare** e **ampliare** le funzionalità di **DetectiveAttacks**, si prevede di implementare nuove caratteristiche e tecnologie in futuro. Uno degli obiettivi principali è facilitare l'utilizzo delle tecnologie attuali all'interno del software, permettendo una gestione più agevole ed efficiente delle varie minacce rilevate. Questo includerà lo sviluppo di strumenti di automazione che **riducano** la necessità di **intervento manuale** da parte degli operatori.

Un altro importante sviluppo futuro sarà l'integrazione di **tecnologie** avanzate per il **riconoscimento** automatico degli indicatori di attacco (**IoA**), in relazione alla previsione già fornita dal sistema riguardante gli attack patterns conosciuti. Questo permetterà al sistema di identificare e analizzare rapidamente le attività sospette, migliorando la capacità di rilevare minacce emergenti e riducendo i tempi di risposta agli incidenti di sicurezza.

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] Michelangelo Sidagni, (2022, 11 Ottobre) Mapping CVEs and ATT&CK Framework TTPs: An Empirical Approach

[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/

[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

[24] 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

[25] MITRE ENGENUITY (2023, 24 Agosto) https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/threat-report-attck-mapper-tram/

[26] Ehsan Aghaei, Ehab Al-Shaer (2023, 6 Settembre)
CVE-driven attack technique prediction with semantic information extraction and a domain-specific language model

[27] Ehsan Aghaei, Xi Niu, Waseem Shadid, Ehab Al-Shaer (2023, 4 Febbraio)
SecureBERT: A Domain-Specific Language Model for Cybersecurity

[28] Chia-Mei Chen, Jing-Yun Kan, Ya-Hui Ou, Zheng-Xun Cai, Albert Guan (2021)
Threat action extraction using information retrieval

[29] H. Zhang, G. Shen, C. Guo, Y. Cui, and C. Jiang (2021, 4 Febbraio)
Ex-action: Automatically extracting threat actions from cyber threat intelligence report based on multimodal learning

[30] G. Ayoade, S. Chandra, L. Khan, K. Hamlen, and B. Thuraisingham (2018, 18 Ottobre)
Automated threat report classification over multi-source data

[31] E. Hemberg, J. Kelly, M. Shlapentokh-Rothman, B. Reinstadler, K. Xu, N. Rutar, and U.-M. O'Reilly (2023, 1 Ottobre)
Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting

[32] A. Kuppa, L. Aouad, and N.-A. Le-Khac (2021, 17 Agosto)
Linking cve's to mitre att&ck techniques

[33] O. Grigorescu, A. Nica, M. Dascalu, and R. Rughinis (2022, 10 Agosto)
Cve2att&ck: Bert-based mapping of cves to mitre att&ck techniques

[34] B. Ampel, S. Samtani, S. Ullman, and H. Chen (2021, 3 Agosto) Linking common vulnerabilities and exposures to the mitre att&ck framework: A self-distillation approach

[35] Lorenzo Colelli (2024, 1 Maggio) https://github.com/colelli/cvwelib.git

[36] NIST (2022, 20 Settembre) https://nvd.nist.gov/developers/vulnerabilities