

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”

CORSO DI LAUREA IN INFORMATICA



Un sistema Honeypot per l'analisi di attacchi
informatici in ambiente controllato

Tesi di Laurea

Relatore

Prof. Vardanega Tullio

Laureando

Marko Peric

Matricola 2011067

ANNO ACCADEMICO 2024-2025

Ringraziamenti

Padova, Agosto 2025

Marko Peric

Sommario

Il presente elaborato descrive il lavoro svolto durante il periodo di stage, della durata di circa 320 ore, dal laureando Marko Peric presso l'azienda Eurosystem S.p.A. dal 18/06/2024 al 13/08/2025. L'elaborato illustra i processi, le metodologie e gli strumenti impiegati nella progettazione e nello sviluppo di un sistema *honeypot* finalizzato al monitoraggio e alla rilevazione di attività malevole in rete. Il sistema si basa sull'installazione di servizi volutamente vulnerabili su un server Linux Debian, con lo scopo di attirare potenziali attaccanti e analizzarne i comportamenti. I *log* generati dai servizi vengono successivamente raccolti, elaborati e trasferiti in InfluxDB per la loro conservazione, e resi disponibili tramite Grafana per consentire un'analisi e una visualizzazione efficace delle informazioni tramite *dashboard*.

Struttura dell'elaborato

In questa sezione viene presentata la struttura dell'elaborato, illustrando brevemente il contenuto di ciascun capitolo:

Il primo capitolo approfondisce il contesto aziendale in cui si è svolto lo *stage*, fornendo una panoramica completa dell'azienda, dei suoi prodotti e servizi nel settore della cybersecurity, degli strumenti tecnologici utilizzati e dell'organizzazione del team di sicurezza informatica, analizzando inoltre l'approccio dell'azienda verso l'innovazione tecnologica;

Il secondo capitolo identifica e analizza il problema alla base del progetto, definendo gli obiettivi specifici dello sviluppo del sistema *honeypot*, i vincoli operativi e tecnici che hanno influenzato il lavoro, le prospettive di

sviluppo futuro e le motivazioni personali che hanno guidato la scelta di questo percorso di stage;

Il terzo capitolo documenta l'intero processo di sviluppo del sistema honeypot, dall'analisi dei requisiti e dei casi d'uso alla progettazione dell'architettura, dalla fase di codifica alle attività di verifica e validazione, presentando il prodotto finale e valutando il grado di conformità rispetto ai requisiti iniziali;

Il quarto capitolo presenta una valutazione retrospettiva dell'esperienza formativa, analizzando il raggiungimento degli obiettivi prefissati, le conoscenze tecniche acquisite nel campo della sicurezza informatica e le competenze professionali sviluppate durante il periodo di tirocinio presso l'azienda.

Criteri tipografici adottati

Riguardo la stesura del testo, relativamente al elaborato sono state adottate le seguenti convenzioni tipografiche:

- gli acronimi e le abbreviazioni sono raccolti in un'apposita sezione dedicata, denominata [Elenco degli acronimi](#) e sono segnati con la seguente nomenclatura *Esempio di acronimo (ES)_G*;
- i termini ambigui o di uso non comune, invece, sono definiti all'interno del [Glossario](#) e sono segnati con la seguente nomenclatura *esempio di termine_G*;
- i termini in lingua straniera o facenti parti del gergo tecnico sono evidenziati con il carattere *corsivo*.

Indice

1	Contesto lavorativo	1
1.1	L'azienda	1
1.2	Prodotti e servizi offerti	2
1.3	Strumenti <i>hardware</i>	4
1.4	Strumenti <i>software</i>	5
1.4.1	Strumenti organizzativi	5
1.4.2	Strumenti produttivi	5
1.5	Organizzazione del team	7
1.5.1	<i>Chief Information Security Officer</i> (CISO)	7
1.5.2	<i>Penetration tester</i>	7
1.5.3	<i>Security analyst</i>	7
1.6	Predisposizione all'innovazione	8
2	Scopo del progetto	12
2.1	Il ruolo dei tirocini in Eurosystem S.p.A.	12
2.2	Analisi del problema	13
2.3	Obiettivi	14
2.4	Vincoli	14
2.5	Sviluppi successivi allo <i>stage</i>	14
2.6	Motivazioni personali	14
3	Sviluppo del progetto	15
3.1	Analisi dei requisiti	15
3.1.1	Casi d'uso	15
3.1.2	Requisiti	15

3.2	Progettazione	15
3.2.1	Architettura del sistema	15
3.2.2	Scelta dei servizi del sistema	16
3.3	Codifica	16
3.3.1	Struttura del progetto	16
3.3.2	Difficoltà incontrate	16
3.4	Verifica	16
3.4.1	Test	16
3.5	Validazione	16
3.6	Risultati del progetto	17
3.6.1	Prodotto finale	17
3.6.2	Conformità ai requisiti	17
4	Valutazione retrospettiva	i
4.1	Obiettivi raggiunti	i
4.2	Conoscenze acquisite	i
4.3	Competenze professionali acquisite	i
	Bibliografia	ii
	Sitografia	iii
	Acronimi e abbreviazioni	iv
	Glossario	v

Elenco delle figure

1.1	Schema di esempio di un processo di penetration testing.	3
1.2	Schema di esempio di un processo di gestione degli endpoint. . .	4
1.3	Dispositivo USB Rubber Ducky. Fonte: https://shop.hak5.org	9
1.4	Dispositivo LAN Turtle. Fonte: https://shop.hak5.org	10

Elenco delle tabelle

Elenco dei codici sorgenti

Capitolo 1

Contesto lavorativo

Il primo capitolo fornisce una panoramica sull'azienda ospitante Eurosystem S.p.A., evidenziando le principali aree operative dell'azienda.

1.1 L'azienda

Eurosystem S.p.A. è un'impresa informatica con sede principale a Villorba (TV), attiva nel settore della consulenza, dei prodotti e dei servizi IT. L'azienda è presente sul territorio nazionale con otto sedi operative, distribuite principalmente nel Nord Italia. Tra queste, la sede di Tavagnacco (UD) riveste un ruolo centrale in quanto ospita il reparto dedicato alle attività di *cybersecurity*, ambito in cui è stato svolto il tirocinio curricolare in modalità da remoto. Fondata con l'obiettivo di fornire soluzioni tecnologiche a supporto delle imprese, Eurosystem S.p.A. si rivolge prevalentemente al settore delle piccole e medie imprese, accompagnandole nei processi di digitalizzazione e nella gestione dei rischi informatici. L'azienda si caratterizza per un approccio che combina l'adozione di tecnologie consolidate con l'attenzione verso l'innovazione e la sicurezza delle infrastrutture digitali. Il reparto di *cybersecurity* si distingue per la sua funzione trasversale, in quanto collabora sia con i clienti sia con gli altri reparti aziendali, integrando misure di protezione all'interno delle soluzioni tecnologiche fornite. L'attenzione di Eurosystem S.p.A. non è rivolta unicamente alla fornitura di servizi, ma anche al mantenimento e all'aggiornamento costante delle competenze del personale. La formazione continua rappresenta un elemento fondamentale:

nei periodi di minore operatività, i team dedicano tempo allo studio di nuove tematiche, all'analisi di strumenti emergenti e alla sperimentazione di metodologie utili a fronteggiare l'evoluzione costante delle minacce informatiche.

1.2 Prodotti e servizi offerti

Eurosystem S.p.A. offre una gamma di prodotti e servizi informatici pensati per garantire la protezione delle infrastrutture IT aziendali. In particolare, il reparto di *cybersecurity* si occupa di diverse attività fondamentali per la difesa e la continuità operativa delle organizzazioni.

Un primo ambito riguarda **il monitoraggio e la risposta agli incidenti**. Attraverso il *Security Operation Center (SOC)_G* e i servizi di *Managed Detection and Response (MDR)_G* viene assicurato un controllo costante delle reti aziendali, con l'obiettivo di rilevare in tempo reale anomalie e potenziali minacce. Ogni incidente viene esaminato nel dettaglio mediante la raccolta e l'analisi dei log e dei dati di rete, l'identificazione dei vettori di attacco e delle vulnerabilità sfruttate, l'isolamento delle minacce e il ripristino dei sistemi tramite soluzioni di *backup* e *disaster recovery*. A completamento del processo, vengono redatti report dettagliati contenenti analisi, azioni intraprese e raccomandazioni di miglioramento.

Un secondo ambito è rappresentato dalle **verifiche di sicurezza**, svolte tramite attività di *Cyber Analysis Assessment*. In questa fase rientrano il *Vulnerability Management* e i *Penetration Test*, strumenti fondamentali per individuare e valutare i punti deboli delle infrastrutture IT. A ciò si affiancano i servizi di *Phishing Assessment*, utili a misurare la resilienza degli utenti contro campagne fraudolente, e le attività di *Threat Intelligence*, finalizzate a raccogliere e analizzare informazioni utili a prevenire attacchi futuri.

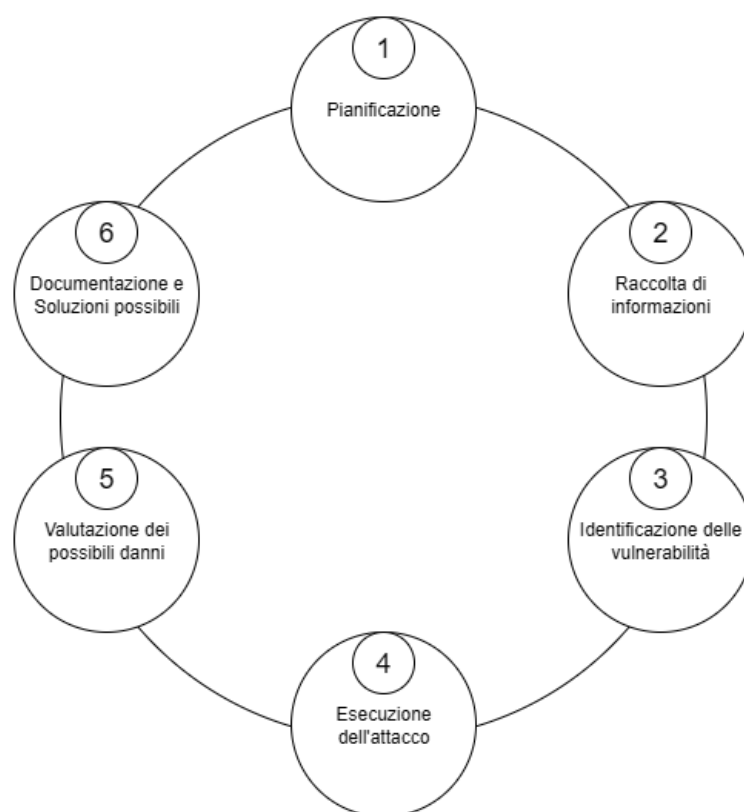


Figura 1.1: Schema di esempio di un processo di penetration testing.

L'analisi delle reti rappresenta un aspetto importante delle attività svolte. Questa comprende il monitoraggio del traffico di rete, il rilevamento di anomalie e la gestione degli eventi di sicurezza, con particolare attenzione alle reti industriali, al fine di contribuire alla continuità operativa dei processi produttivi.

Un ruolo centrale è svolto anche dalla **gestione degli endpoint**, ossia la protezione dei dispositivi aziendali, interni o remoti. Questa attività comprende il monitoraggio costante dello stato di sicurezza, l'applicazione degli aggiornamenti correttivi e delle politiche di protezione, il controllo delle identità e degli accessi, nonché il rilevamento e la risposta rapida alle minacce. Inoltre, sono previsti report e *audit* di conformità, volti a garantire trasparenza e allineamento con le normative.

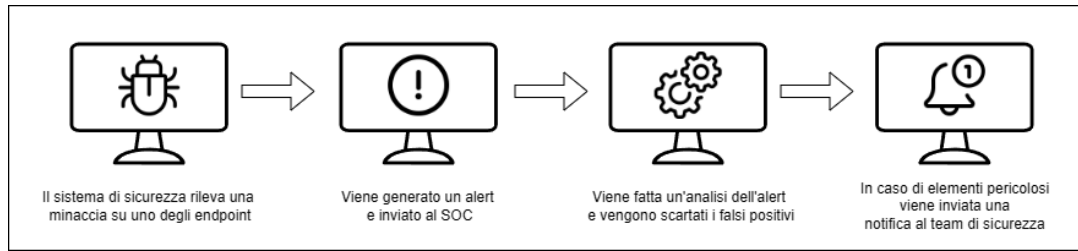


Figura 1.2: Schema di esempio di un processo di gestione degli endpoint.

Alla gestione degli endpoint si affianca la **gestione dei dati**. Eurosystem supporta le aziende nella protezione, nell'organizzazione e nella conformità dei dati, in linea con i requisiti normativi, assicurando così un trattamento sicuro e affidabile delle informazioni.

Un altro elemento di rilievo è la **gestione degli utenti e la sensibilizzazione**. L'azienda promuove attività formative mirate a diffondere buone pratiche di sicurezza informatica, con particolare attenzione agli accessi, ai privilegi e ai comportamenti corretti. In questo modo viene ridotto il rischio legato al fattore umano, spesso determinante nella riuscita di un attacco informatico.

Infine, Eurosystem offre un **supporto tempestivo in caso di criticità**. In presenza di incidenti o sospette violazioni, i clienti ricevono un'assistenza diretta e immediata, con l'obiettivo di ridurre al minimo l'impatto sull'operatività aziendale. Grazie a questo insieme di attività, l'azienda è in grado di identificare proattivamente le vulnerabilità dei sistemi informativi, predisporre misure di protezione adeguate e garantire un aggiornamento costante delle competenze necessarie per affrontare l'evoluzione delle minacce informatiche.

1.3 Strumenti *hardware*

Nel caso in cui le attività lavorative vengano svolte da remoto, l'azienda mette a disposizione del lavoratore gli strumenti necessari per garantire il corretto svolgimento delle mansioni assegnate. In particolare, viene fornito un computer portatile HP, configurato con l'account e la casella di posta elettronica azienda-

le, così da assicurare l'accesso immediato a tutte le risorse interne. A supporto dell'utilizzo del dispositivo, è inoltre fornito un mouse.

1.4 Strumenti *software*

Le tecnologie e gli strumenti software a supporto delle attività lavorative si articolano principalmente in due grandi categorie: strumenti organizzativi e strumenti produttivi.

1.4.1 Strumenti organizzativi

Per quanto riguarda gli strumenti organizzativi, l'azienda fa ampio uso di ***Microsoft Teams***, che rappresenta il principale canale di comunicazione interna. Questo strumento consente di coordinare le attività quotidiane, condividere documenti in modo rapido ed efficace e partecipare a riunioni o chiamate di lavoro quando necessario.

Un ruolo altrettanto centrale è ricoperto da ***Microsoft Outlook***, utilizzato non solo per la gestione della posta elettronica e dell'agenda, ma anche per la pianificazione di incontri e il mantenimento di un flusso di comunicazione costante, sia con i colleghi che con i clienti. Outlook svolge inoltre una funzione cruciale nella ricezione di notifiche riguardanti incidenti di sicurezza provenienti da aziende esterne, garantendo così risposte tempestive in caso di necessità.

A completare questo insieme di strumenti organizzativi vi è ***GitHub***, adottato come piattaforma di controllo versione. Questo strumento consente la gestione strutturata del codice sorgente, il tracciamento delle modifiche e la collaborazione efficiente tra più sviluppatori.

1.4.2 Strumenti produttivi

Sul versante degli strumenti produttivi, un ruolo rilevante è svolto da ***LaTeX***, scelto per la redazione di documentazione tecnica e scientifica grazie alle

sue elevate capacità di formattazione. La possibilità di gestire con precisione formule matematiche, grafici, bibliografie e glossari permette di ottenere documenti di elevata qualità tipografica. Il modello di separazione tra contenuto e presentazione rende inoltre il codice sorgente facilmente riutilizzabile e particolarmente adatto a contesti di collaborazione accademica e professionale.

In parallelo, l'azienda fa un ampio utilizzo di ***Python***, linguaggio di programmazione versatile e diffuso, applicato soprattutto nel settore della *cybersecurity*. Le sue potenzialità vengono sfruttate per automatizzare processi, analizzare file di log e sviluppare strumenti di monitoraggio e rilevamento delle minacce, anche grazie alle numerose librerie specializzate che semplificano la creazione di script per il testing della sicurezza, l'interazione con *Application Programming Interface (API)*_G e la gestione di sistemi complessi.

A supporto dello sviluppo viene frequentemente adottato ***Visual Studio Code (VSCode)***, un ambiente di programmazione leggero, modulare e altamente personalizzabile. Questo strumento è impiegato principalmente per la scrittura, il debugging e la manutenzione del codice, offrendo un'ampia compatibilità con diversi linguaggi e la possibilità di integrare estensioni dedicate. Pur essendo l'IDE più diffuso tra i dipendenti, la sua adozione non è vincolante: ciascun lavoratore può infatti optare per soluzioni alternative in base alle proprie esigenze e preferenze operative.

Infine, un ulteriore strumento di grande rilevanza è ***Docker***, una tecnologia di virtualizzazione basata sui *container*. Grazie a questo approccio, è possibile creare ambienti isolati, scalabili e facilmente replicabili, in cui le applicazioni vengono eseguite includendo tutte le dipendenze necessarie. La leggerezza e portabilità della tecnologia ne favoriscono l'uso in fase di sviluppo, testing e distribuzione, riducendo al minimo i problemi di compatibilità tra diversi sistemi.

1.5 Organizzazione del team

1.5.1 *Chief Information Security Officer (CISO)*

Il *Chief Information Security Officer (CISO)*_G è la figura responsabile della strategia di sicurezza informatica all'interno dell'azienda. Supervisiona tutte le attività del reparto di *cybersecurity* e ne garantisce la coerenza con gli obiettivi aziendali e con le normative vigenti. Durante il periodo di tirocinio, questa figura ha ricoperto anche il ruolo di tutor aziendale, fornendo supporto e guida nelle varie attività. Tra le sue principali responsabilità rientrano la definizione delle politiche e delle strategie di sicurezza, la supervisione delle attività operative del team, il coordinamento tra i diversi ruoli del reparto e la verifica della conformità agli standard di settore. A ciò si aggiunge un impegno costante nel supporto e nella formazione interna, volto a diffondere buone pratiche di sicurezza informatica tra i dipendenti.

1.5.2 *Penetration tester*

Il *penetration tester* ha l'obiettivo di individuare le vulnerabilità presenti nei sistemi informatici attraverso l'esecuzione di attacchi simulati in un contesto controllato. Il suo lavoro si articola in più fasi, che comprendono la pianificazione e l'esecuzione di *penetration test*, la simulazione di scenari di attacco realistici e l'analisi delle debolezze riscontrate. Al termine delle attività, il professionista redige report tecnici dettagliati nei quali vengono descritte le criticità emerse, corredati da proposte di contromisure e raccomandazioni operative, così da supportare l'azienda nell'adozione di strategie efficaci di mitigazione del rischio.

1.5.3 *Security analyst*

Il *security analyst* si occupa del monitoraggio costante dei sistemi informativi e della gestione operativa degli eventi di sicurezza, con l'obiettivo di rilevare tempestivamente potenziali incidenti e coordinare una risposta adeguata. Le sue attività comprendono il controllo delle infrastrutture tramite strumenti avanzati

di analisi, il rilevamento e la classificazione degli avvisi di sicurezza, nonché l'esame dei log e delle anomalie di rete. In caso di incidenti, fornisce supporto operativo nelle attività di risposta e contribuisce alla definizione di procedure correttive. Inoltre, elabora linee guida e buone pratiche da condividere con clienti e colleghi, contribuendo così a diffondere una maggiore consapevolezza in materia di sicurezza informatica.

1.6 Predisposizione all'innovazione

L'ambito della *cybersecurity* è caratterizzato da un'evoluzione continua: nuove vulnerabilità, strumenti di attacco e metodologie di compromissione emergono con frequenza sempre maggiore. Per questo motivo, l'innovazione e l'aggiornamento costante costituiscono elementi fondamentali per ogni azienda che operi in questo settore. Eurosystem S.p.A. ha sviluppato un approccio che integra formazione, ricerca e sperimentazione, con l'obiettivo di anticipare i rischi e fornire soluzioni di difesa sempre più efficaci ai propri clienti. Un aspetto centrale è la formazione continua: nei momenti di minore operatività i team si dedicano allo studio di nuove tematiche, alla valutazione di strumenti emergenti e all'adozione di metodologie innovative. In questo modo rimangono aggiornati sull'evoluzione delle minacce informatiche e rafforzano le proprie competenze tecniche. In parallelo, viene dato ampio spazio alla sperimentazione pratica di strumenti e tecniche di attacco. L'azienda valuta regolarmente soluzioni utilizzate dai *penetration tester* durante le verifiche di sicurezza sui sistemi dei clienti. Tra questi strumenti rientrano dispositivi come:

- **USB Rubber Ducky**, che permette di eseguire comandi automatici sui dispositivi a cui viene collegata, simulando un attacco tramite periferica USB. Viene impiegata per facilitare le attività di *penetration testing* in loco presso le aziende clienti, consentendo di valutare la sicurezza delle postazioni di lavoro rispetto a questo tipo di minacce;



Figura 1.3: Dispositivo USB Rubber Ducky.

Fonte: <https://shop.hak5.org>

- **LAN Turtle**, un adattatore di rete che consente di instaurare accessi remoti nascosti e di analizzare il traffico direttamente dall'interno della rete aziendale. Viene utilizzato durante le attività di *penetration testing* per verificare l'esposizione delle infrastrutture a minacce derivanti dall'inserimento fisico di dispositivi malevoli;



Figura 1.4: Dispositivo LAN Turtle.
Fonte: <https://shop.hak5.org>

L'adozione di tali strumenti non ha un fine puramente dimostrativo, ma rappresenta un'attività concreta di valutazione del livello di sicurezza dei clienti, in quanto permette di evidenziare vulnerabilità legate al fattore umano e alla protezione fisica delle postazioni di lavoro. Oltre agli strumenti hardware, vengono analizzate e adottate nuove piattaforme e metodologie orientate sia all'offensiva sia alla difensiva. Tra queste si possono citare:

- l'impiego di tecniche avanzate di *Threat Intelligence*, volte a raccogliere e analizzare informazioni relative a campagne malevole, infrastrutture di attacco e nuove vulnerabilità sfruttate in scenari reali;
- l'aggiornamento continuo dei framework di *penetration testing* e *vulnerability management*, che consente di disporre di strumenti più precisi ed efficaci per identificare punti deboli e priorità di intervento;

- la sperimentazione di approcci innovativi al *red teaming*, in cui vengono simulate operazioni complesse di attacco, con l'obiettivo di valutare non soltanto le difese tecnologiche ma anche le capacità organizzative e di risposta dei clienti.

In conclusione, la predisposizione all'innovazione non è intesa come un'attività separata, ma come parte integrante delle operazioni quotidiane. L'integrazione di formazione, sperimentazione e ricerca applicata consente al reparto di *cybersecurity* di affrontare in maniera proattiva le sfide poste dalle minacce informatiche, mantenendo un equilibrio tra lo sviluppo delle competenze interne e l'offerta di servizi sempre più efficaci e aggiornati per i clienti.

Capitolo 2

Scopo del progetto

Il secondo capitolo descrive il ruolo degli stage nel contesto aziendale e come questo abbia portato alla definizione degli obiettivi del progetto. Inoltre vengono analizzati i vincoli e le motivazioni personali che hanno influenzato lo sviluppo del progetto stesso.

2.1 Il ruolo dei tirocini in Eurosystem S.p.A.

Eurosystem S.p.A. considera i tirocini un elemento strategico sia per la formazione dei giovani sia per l'innovazione aziendale nel settore della *cybersecurity*. Essi permettono di avvicinarsi concretamente al mondo del lavoro e di contribuire ai progetti aziendali. L'azienda non interpreta il tirocinio soltanto come un'esperienza formativa, ma anche come un'opportunità per sperimentare nuove idee di progetto e per valutare soluzioni tecnologiche che, se ritenute efficaci, possono essere integrate nei servizi offerti ai clienti con l'obiettivo di rafforzarne la sicurezza informatica. I tirocinanti vengono accolti in un contesto lavorativo dinamico, caratterizzato da attività concrete e da un costante confronto con professionisti del settore. Fin dal loro inserimento, hanno la possibilità di applicare le conoscenze già acquisite e di arricchirle con competenze operative, maturate direttamente a contatto con problematiche reali della *cybersecurity*. Questa modalità consente non solo di consolidare il proprio bagaglio tecnico, ma anche di sviluppare capacità trasversali come la collaborazione, la creatività e il *problem solving*, indispensabili per affrontare scenari complessi e in con-

tinua evoluzione. Il tirocinio assume così un ruolo bidirezionale: da un lato favorisce la crescita formativa e professionale del tirocinante, dall'altro rappresenta per Eurosystem un'occasione per esplorare nuove prospettive progettuali e per individuare talenti da coinvolgere attivamente nelle sfide della sicurezza informatica.

2.2 Analisi del problema

Uno dei principali problemi che le organizzazioni si trovano ad affrontare riguarda la capacità di **individuare tempestivamente attività malevole** all'interno dei propri sistemi. La sicurezza informatica rappresenta oggi una delle sfide più complesse per le aziende di qualsiasi settore. Le infrastrutture IT moderne sono caratterizzate da un'elevata interconnessione e da una crescente dipendenza da servizi digitali, fattori che le rendono esposte a minacce sempre più sofisticate. Gli attacchi informatici non sono più episodi sporadici, ma eventi ricorrenti che possono compromettere la continuità operativa, causare perdite economiche e danneggiare in modo significativo la reputazione aziendale.

Le tecniche di attacco evolvono rapidamente e gli strumenti difensivi tradizionali, come firewall e antivirus, non sempre riescono a garantire una protezione completa. Gli aggressori, infatti, sfruttano vulnerabilità sconosciute, configurazioni errate o semplicemente il fattore umano, riuscendo così ad aggirare i controlli di sicurezza.

A ciò si aggiunge la difficoltà di comprendere a fondo il comportamento degli attaccanti. Spesso le aziende hanno una visibilità limitata su quali metodi vengano impiegati, su come gli aggressori si muovano una volta ottenuto l'accesso e su quali siano gli obiettivi finali delle intrusioni. Questa mancanza di informazioni rende complesso elaborare strategie di difesa realmente efficaci e impedisce di anticipare possibili minacce future.

In sintesi, il problema principale è legato all'**assenza di strumenti e metodologie** che consentano non solo di rilevare gli attacchi, ma anche di comprenderne le dinamiche e trarne conoscenza utile per migliorare la sicurezza complessiva dei sistemi informativi.

2.3 Obiettivi

Questa sezione definisce gli obiettivi specifici dello *stage* accordati con il tutor aziendale, stabilendo risultati misurabili e traguardi concreti da raggiungere durante il periodo di tirocinio.

2.4 Vincoli

Questa sezione identifica i vincoli tecnici, temporali e organizzativi che hanno influenzato lo sviluppo del progetto, spiegando come questi sono stati gestiti durante lo *stage*.

2.5 Sviluppi successivi allo *stage*

Si descrivono le possibili evoluzioni future del progetto sviluppato durante lo *stage* e come questo potrà essere integrato e sviluppato ulteriormente dall'azienda.

2.6 Motivazioni personali

Descrive le motivazioni personali che hanno spinto alla scelta di questo stage, gli interessi specifici nel campo della *cybersecurity* e le aspettative di crescita professionale.

Capitolo 3

Sviluppo del progetto

3.1 Analisi dei requisiti

3.1.1 Casi d'uso

Vengono identificati e descritti i principali casi d'uso del sistema sviluppato, illustrando gli scenari operativi in cui il prodotto sarà utilizzato e le interazioni tra utenti e sistema.

3.1.2 Requisiti

Si presenta l'analisi completa dei requisiti funzionali e non funzionali del sistema, definendo le specifiche tecniche che la soluzione deve soddisfare per rispondere alle esigenze aziendali.

3.2 Progettazione

3.2.1 Architettura del sistema

Viene descritta l'architettura complessiva del sistema sviluppato, illustrando la struttura dei componenti, le loro interazioni e le scelte architetturali tramite diagrammi delle classi e diagrammi di flusso.

3.2.2 Scelta dei servizi del sistema

Questa sezione illustra le motivazioni alla base della selezione dei servizi vulnerabili inclusi nel progetto, evidenziando come ciascuno di essi contribuisca al sistema.

3.3 Codifica

3.3.1 Struttura del progetto

Viene presentata l'organizzazione del codice e dei file del progetto, descrivendo la struttura delle cartelle, i pattern di sviluppo utilizzati e le convenzioni adottate per garantire manutenibilità e leggibilità.

3.3.2 Difficoltà incontrate

La sezione analizza gli ostacoli incontrati durante lo sviluppo del progetto, sia di natura tecnica sia organizzativa. Viene descritto come ciascuna difficoltà sia stata gestita e superata, evidenziando le soluzioni adottate.

3.4 Verifica

3.4.1 Test

La sezione illustra il metodo seguito per condurre le attività di testing, descrivendo i diversi tipi di test implementati e gli strumenti utilizzati per garantire la qualità del software.

3.5 Validazione

In questa sezione si illustra il processo di validazione del progetto sviluppato, includendo i test con strumenti di controllo e la verifica del rispetto dei requisiti.

3.6 Risultati del progetto

3.6.1 Prodotto finale

Questa sezione descrive il prodotto ottenuto dallo stage e come questo funziona, nei suoi vari aspetti e funzionalità.

3.6.2 Conformità ai requisiti

In questa sezione viene analizzato il grado di soddisfacimento dei requisiti inizialmente identificati, evidenziando quali requisiti sono stati raggiunti completamente e quali potrebbero richiedere sviluppi futuri.

Capitolo 4

Valutazione retrospettiva

4.1 Obiettivi raggiunti

La sezione ha l'obiettivo di fornire una valutazione dettagliata dei risultati ottenuti durante lo *stage*, evidenziando quali e quanti degli obiettivi precedentemente definiti siano stati effettivamente raggiunti.

4.2 Conoscenze acquisite

Questa sezione elenca e descrive le nuove conoscenze acquisite durante lo stage, particolare riferimento alle tecnologie, metodologie e tecniche nel campo della cybersecurity e dello sviluppo *software*.

4.3 Competenze professionali acquisite

In questa sezione si descrivono le competenze pratiche e professionali sviluppate durante l'esperienza di *stage*, incluse competenze tecniche specifiche, capacità di *problem solving* e abilità di lavoro in team in ambiente professionale.

Bibliografia

Sitografia

Acronimi e abbreviazioni

API *Application Programming Interface.* [6](#)

CISO *Chief Information Security Officer.* [7](#)

ES Esempio di acronimo. [v](#)

MDR *Managed Detection and Response.* [2](#)

SOC *Security Operation Center.* [2](#)

Glossario

Audit Un processo sistematico di esame e valutazione delle attività, dei controlli e delle procedure di un'organizzazione, al fine di garantire la conformità alle normative e l'efficacia delle misure di sicurezza. [3](#)

Esempio di nome Esempio di descrizione. [v](#)