Università degli studi di Modena e Reggio Emilia
Dipartimento di Scienze Fisiche, Informatiche e Matematiche

Corso di Laurea in Informatica

Valutazione di tecnologie innovative per il monitoraggio della sicurezza delle reti

Relatore:
Prof. Ferretti Luca

Candidato:
Violi Matteo

Anno Accademico 2023/2024

Indice

Capitolo 1

Introduzione

Nell'ambito della sicurezza informatica, una delle sfide principali è l'identificazione tempestiva e l'analisi approfondita delle minacce. Le organizzazioni, pubbliche e private, devono affrontare l'inevitabile complessità delle reti, la diversità delle minacce sia interne che esterne alla rete privata. Ciò in quanto la mancanza di strumenti efficaci per il rilevamento delle intrusioni e la gestione delle minacce può portare a vulnerabilità e rischi per la sicurezza.
IBM stima che nel 2023 il costo medio di un data breach è di 4,5 milioni di dollari americani. In questo contesto, dove le minacce cibernetiche sono in costante evoluzione, diventa cruciale sviluppare e implementare metodologie avanzate per proteggere i dati, gli utenti, i dispositivi e le reti dalle intrusioni, utilizzando tecniche proattive per rilevare, prevenire e rispondere agli attacchi informatici.
Tra esse è possibile annoverare l'utilizzo di un honeypot, come T-Pot, oppure di un IDPS, come Darktrace. Questi sistemi, approfonditi nel presente lavoro, sono stati utilizzati durante l'esperienza di tirocinio al fine di mitigare minacce interne ed esterne alla rete interna.
Rispetto alle soluzioni tradizionali, che si basano principalmente su firewall per il perimetro esterno e policy di routing e VLAN per il perimetro interno, l'implementazione di un honeypot e lo studio delle possibili minacce rilevabili tramite IDPS durante il tirocinio offrono una maggiore visibilità delle minacce in tempo reale. Ciò consente una risposta più rapida e mirata agli attacchi, grazie all'integrazione di IDPS e honeypot, aumenta la possibilità di prevenire incidenti tramite la deviazione di attacchi nel caso sia al di fuori del perimetro o tramite il monitoraggio della rete nel caso sia all'interno.
Attraverso la sperimentazione dell'honeypot verranno descritte le principali minacce e vettori di attacco nel mondo della sicurezza informatica, inoltre grazie a Darktrace verranno esaminati diversi potenziali scenari di attacco e problemi giornalieri specificando le procedure per mitigare i rischi.
Il lavoro svolto si concentra sulla ricerca di soluzioni pratiche e efficaci per affrontare le sfide sempre crescenti nel campo della sicurezza informatica, fornendo un contributo significativo alla prevenzione di possibili attacchi e alla diminuzione del traffico malevolo su sistemi in uso.

Nel capitolo 2 viene esaminata la teoria relativa agli honeypot e agli IDS, approfondendo le definizioni e le tipologie esistenti. Si analizzano poi in dettaglio le piattaforme utilizzate per implementare tali concetti.
Nel capitolo 3 vengono esplorati gli utilizzi pratici delle suddette piattaforme,

includendo configurazioni, dati raccolti e esempi di attacchi rilevati.
Infine, nel capitolo 4 viene presentata la conclusione, riassumendo le principali scoperte e riflessioni emerse durante lo studio e l'implementazione delle soluzioni discusse.

Capitolo 2

Fondamenti teorici su Honeypot e IDS

Nella sezione 2.1 di questo capitolo vengono delineate le fondamenta degli honeypot, includendo la loro definizione e origine (2.1.1), le varie tipologie esistenti (2.1.2), un'analisi teorica approfondita di T-Pot con un'occhiata tecnica (2.1.3) e una chiara esposizione degli obiettivi del tirocinio (2.1.4).
Nella sezione 2.2 del capitolo, si approfondisce la definizione e la storia degli IDS (2.2.1), seguita da una panoramica dettagliata di Darktrace (2.2.2), l'IDPS utilizzato. Successivamente, viene fornita un'analisi approfondita sul funzionamento di Darktrace (2.1.3)(2.1.4).

2.1 Introduzione agli honeypot

2.1.1 Definizione e origine degli honeypot

Un honeypot, come definito dal NIST (National Institute of Standards and Technology), è un sistema o una risorsa del sistema che è progettata per attrarre potenziali *cracker* e *intrusori*, il concetto alla base è quello di impiantare deliberatamente in un sistema apparenti vulnerabilità con lo scopo di rilevare attacchi e confondere i possibili attaccanti su quali vulnerabilità sfruttare[1].
Lance Spitzner, direttore del SANS Institute, pone come origine degli honeypot due opere pubblicate quasi simultaneamente[2]. La prima risale al 1989, quando Clifford Stoll pubblicò il romanzo *The Cuckoo's Egg*, destinato a diventare uno dei classici della letteratura in materia di sicurezza informatica, nel quale racconta di come aveva scoperto un tentativo di intrusione informatica nei sistemi del Lawrence Berkeley National Laboratory, dove lavorava come astrofisico. In particolare, egli aveva notato discrepanze nelle fatture di addebito per l'uso di risorse informatiche e aveva cercato di capirne la causa, seguendo le tracce digitali lasciate, le quali lo condussero fino ad un hacker. Quest'ultimo si rivelò essere Markuss Hess, hacker tedesco, noto per aver violato più di quattrocento sistemi dell'esercito americano, per poi vendere le informazioni ai servizi di intelligence sovietici. Hess venne scoperto grazie a un'idea di Stoll: un finto portale vulnerabile del Lawrence Berkeley National Laboratory. Quest'ultimo gli permise di stabilire una connessione e localizzare il criminale. Stoll definì questa sua creazione una hoax, una sorta di burla o truffa[3].

Il secondo documento fondante sull'uso di trappole per attirare hacker malevoli fu redatto da William Cheswick, un pioniere della sicurezza informatica e l'ideatore di uno dei primi firewall. Cheswick creò quello che in quell'epoca lui chiamò roach motel, letteralmente "motel per scarafaggi", una trappola progettata per intrappolare gli hacker[4].
Nel 1997, Fred Cohen ha pubblicato il Deception Toolkit (DTK) per la comunità della sicurezza informatica, fornendo una solida struttura di base per la creazione dei moderni honeypot. Successivamente, nel 1998, è stato rilasciato il Cybercop Sting, il primo honeypot ad uso commerciale progettato per essere installato su macchine della famiglia Windows NT e simulare una rete reale[2].
Nel corso degli anni, il termine *honeypot* ha guadagnato sempre più popolarità, in quanto associato alla tradizione folkloristica dei popoli germanici[5], slavi e celtici, secondo cui gli orsi tendono a rubare il miele dagli alveari, metafora che riflette l'idea di attirare e intrappolare gli 'hacker' simili a predatori.
Secondo Lance Spitzner, un honeypot può essere molto utile poiché ricopre i tre paradigmi della sicurezza informatica: prevenzione, rilevamento e risposta. Serve per la prevenzione poiché il suo obiettivo è quello di attirare e distogliere l'attenzione di un potenziale attaccante dai sistemi realmente utilizzati. È utile al rilevamento in quanto consente di individuare ogni connessione, pacchetto e indirizzo IP che si collega ad esso. Inoltre, è fondamentale per la risposta: in primo luogo, perché qualsiasi attore malevolo collegatosi può essere successivamente bloccato da un firewall; in secondo luogo, perché analizzando i comportamenti degli attaccanti è possibile comprendere meglio i vettori di attacco[2].

2.1.2 Tipologie di honeypot

È possibile categorizzare le diverse tipologie di honeypot in base alle risorse allocate o al contesto di utilizzo. Secondo Iyatiti Mokube e Michele Adams, professori presso la Armstrong Atlantic State University, in base al contesto di utilizzo è possibile distinguere[6]:

- **Honeypot di Produzione**: i quali sono progettati per un utilizzo semplice, immagazzinano un numero limitato di informazioni e sono spesso implementati in contesti aziendali. Collocati all'interno della rete aziendale insieme agli altri server di produzione, raccolgono meno dati e operano a bassa intensità[7].

- **Honeypot di Ricerca**: i quali sono finalizzati alla raccolta di informazioni sulle metodologie di attacco degli aggressori. Non forniscono un valore specifico a un'organizzazione particolare, ma sono più complessi da installare e mantenere, raccogliendo un'ampia quantità di dati[8].

Per quanto riguarda le risorse, è possibile suddividerli in due categorie principali:

- **Honeypot Fisici**: utilizzano macchine reali con indirizzi IP dedicati, simulando comportamenti modellati dal sistema. Questo modello è raramente adottato a causa dell'alto costo di acquisizione, manutenzione e delle specifiche esigenze hardware.

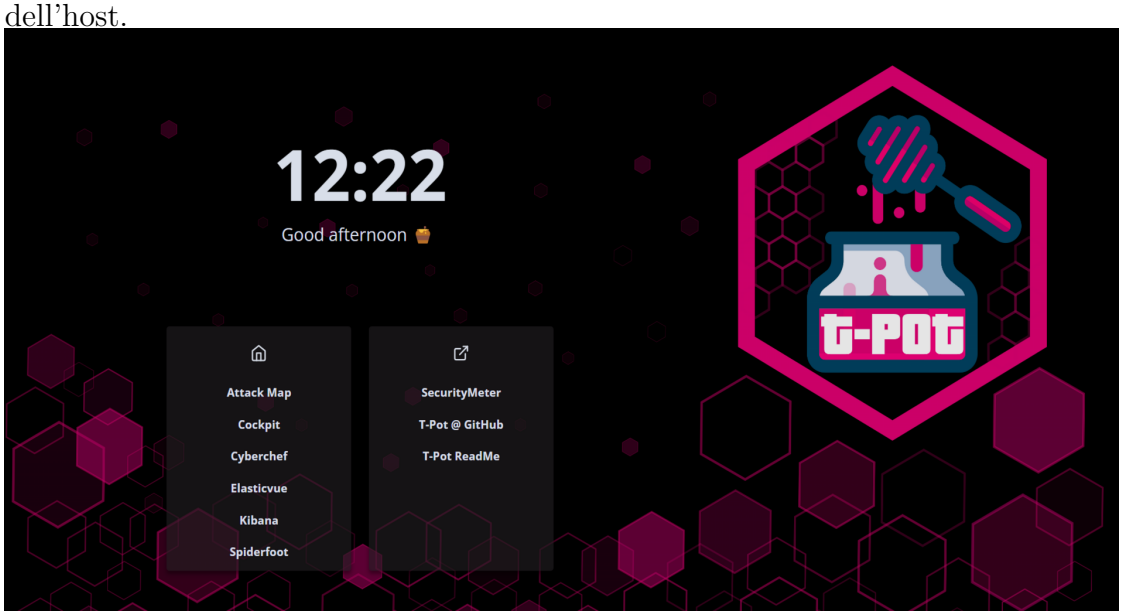
- **Honeypot Virtuali**: consentono l'installazione e la simulazione di un host sulla rete, assegnando un indirizzo IP alla macchina virtuale. È l'approccio più diffuso, offrendo un equilibrio tra efficacia e praticità[9].

Recentemente, il mercato legato a questi servizi ha introdotto nuove tipologie di honeypot che estendano le funzionalità di base e incorporino tecniche di inganno, automatizzando la scalabilità su grandi reti. Le tipologie più diffuse includono:

- **Honeypot malware**: simulano un sistema vulnerabile agli attacchi più comuni da parte di malware, consentendo uno studio approfondito del malware, delle sue origini e del suo comportamento[10].
- **Honeypot spam**: simulano relay di posta aperti o proxy aperti, comunemente utilizzati dagli spammer. Ciò consente di rivelare l'indirizzo IP dello spammer e fornire una cattura in blocco dello spam[11].
- **Honeypot database**: simulano database con possibili vulnerabilità, come ad esempio SQL Injection[12].
- **Honeypot ICS**: simulano sistemi di controllo industriale come i PLC (controller logico programmabile)[13].

2.1.3 Tpot: panoramica

La piattaforma T-Pot, sviluppata da Deutsche Telekom Security GmbH, è distribuita sotto licenza GPL-3.0, un modello copyleft per il software libero. Basata su Debian 11 per architetture amd64 e arm64, utilizza Docker e Docker-compose per eseguire simultaneamente una vasta gamma di strumenti e sfruttare appieno le risorse hardware dell'host.



T-Pot offre una serie di servizi suddivisibili in cinque categorie principali:

1. Connessione tramite SSH e Cockpit per la gestione attraverso un'interfaccia web.
2. Elastic Stack, composto da Elasticsearch per l'archiviazione dei dati, Logstash per l'analisi e Kibana per la visualizzazione su dashboard.

3. Strumenti quali Cyberchef per la codifica e decodifica dei dati, Elasticvue per l'interazione con un cluster Elasticsearch, T-Pot Attack Map per la visualizzazione degli attacchi in tempo reale e Spiderfoot per l'automazione dell'OSINT.

4. Honeypot, che includono una selezione di ventidue honeypot configurabili.

5. Monitoraggio della rete attraverso Suricata, un motore di sicurezza di rete.

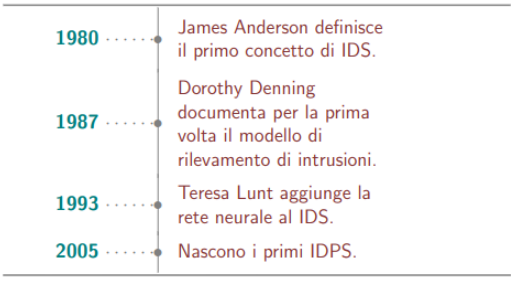
2.1.4 Tpot: scopo e utilità in ambiente di tirocinio

Nel contesto del tirocinio, lo scopo di T-Pot è stato duplice: inizialmente, configurare due tipologie di honeypot in un ambiente di laboratorio per valutare quale fosse la più adatta alle esigenze dell'azienda e comprendere i loro punti di forza e debolezza. Successivamente, il fine era quello di trasferire il modello selezionato in ambiente di produzione, esponendolo alla rete esterna. Le due tipologie testate includono un honeypot *standalone* completo e la creazione di una rete di honeypot che invia dati all'*alveare*, il quale raccoglie e trasferisce i dati a un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM). L'utilità di questo lavoro era ottenere un honeypot in grado di attirare gli attacchi lontano dai sistemi operativi effettivamente utilizzati, con la possibilità di offrire il servizio ai clienti.

2.2 Teoria sugli IDS

2.2.1 Definizione e origine degli IDS

Un IDS (Intrusion Detection System), così definito dal NIST, è un processo di monitoraggio degli eventi che si verificano in un computer o in una rete e dell'analisi di essi per individuare segni di intrusioni, quest'ultime vengono definite come tutti i tentativi di compromettere la confidenzialità, l'integrità, la disponibilità o di aggirare meccanismi di sicurezza di un computer o di una rete[14].



La prima elaborazione del concetto di sistema di IDS risale al 1980 e si deve in particolare a James Anderson, analista presso la National Security Agency. Il sistema di Anderson comprendeva un insieme di strumenti per amministratori di sistema per poter esaminare i registri di audit[15]. Nel febbraio del 1987, Dorothy E. Denning, assistita da Peter G. Neumann presso IDS International, pubblicò un documento intitolato "An Intrusion Detection Model", nel quale introdussero miglioramenti al modello di Anderson[16]. Il modello di Denning consisteva in un sistema esperto basato su regole per rilevare pattern di intrusioni note e una componente di rilevazione statistica basata su profili di utenti, sistemi host e sistemi di destinazione, diventando noto come Intrusion Detection Expert System. Nel 1990, Teresa F. Lunt, autrice di "IDES: An Intelligent System for Detecting Intruders", aggiunse l'ultimo componente al modello di Denning: una rete neurale artificiale capace di adattarsi agli eventi e modificarsi[17].
Un sistema di rilevamento delle intrusioni (IDS) è un dispositivo software o un'applicativo che monitora una rete o i dispositivi su cui è installato. Quando rileva un'anomalia, la segnala a un sistema di raccolta di eventi di sicurezza (SIEM), che utilizza tecniche di filtraggio degli allarmi per distinguere falsi positivi da attività dannose[18].
Gli IDS, come i firewall, vengono utilizzati per bloccare intrusioni nella rete, ma differiscono dalla risposta a tali intrusioni. I sistemi di rilevamento delle intrusioni possono anche avere scopi specifici se integrati con strumenti personalizzati, come l'utilizzo di un honeypot per attirare e caratterizzare il traffico dannoso[19].
Recentemente, sono stati realizzati prodotti denominati sistemi di rilevamento e prevenzione delle intrusioni (IDPS), i quali possiedono la capacità di rispondere proattivamente alle intrusioni rilevate. Gli IDPS hanno, inoltre, la capacità di fermare un attacco rilevato, registrare gli eventi, avvisare gli amministratori, bloccare la minaccia e generare rapporti. A differenza degli IDS, gli IDPS devono essere posizionati "in linea", monitorando in tempo reale per bloccare intrusioni, inviare allarmi, rifiutare pacchetti dannosi e correggere errori di rete[20].

2.2.2 Tipologie di IDS

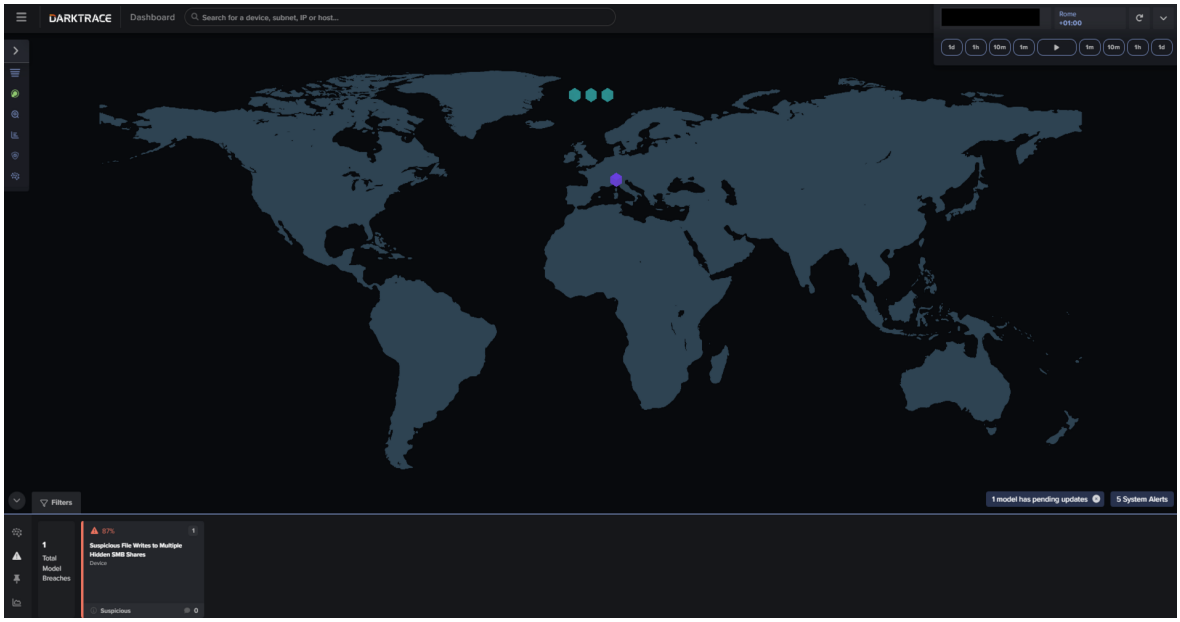
Secondo il NIST è possibile classificare gli IDS in base alla loro posizione o all'approccio di rilevamento, in base alla posizione si dividono in:

- **NIDS (Network IDS)**: posizionati strategicamente nella rete, monitorano il traffico da e verso tutti i dispositivi, analizzando idealmente sia l'entrata che l'uscita. L'uso di reti neurali artificiali può migliorare i tassi di rilevamento grazie alla capacità di analizzare grandi volumi di dati in modo intelligente e apprendere dagli errori, sviluppando un sistema di avviso precoce[18].
- **HIDS (Host IDS)**: operano su singoli host o dispositivi, monitorando solo i pacchetti in entrata e in uscita. Consentono l'analisi del traffico di rete criptato, una volta arrivato all'host[18].

In base all'approccio di rilevamento invece si dividono in:

- **Signature-based**: ricerca pattern specifici, simile all'azione degli antivirus per individuare sequenze di byte o istruzioni malevole conosciute. Risponde velocemente ad attacchi noti, ma può non riconoscere nuovi attacchi senza pattern noti[21].
- **Anomaly-based**: utilizza l'apprendimento automatico per creare un modello di attività affidabile e confrontare il nuovo comportamento. Riesce a rilevare attacchi sconosciuti, ma potrebbe generare falsi positivi, identificando attività legittime come malevoli[22].

2.2.3 Darktrace: panoramica



Darktrace, fondata nel 2013 a Cambridge, Regno Unito, da ex-dipendenti dell'intelligence governativa e matematici dell'Università di Cambridge, è un Intrusion Detection and Prevention System (IDPS) che immagazzina e analizza il traffico di rete per lunghi periodi al fine di identificare correlazioni e modelli comportamentali.
Utilizzando avanzate tecniche di probabilità bayesiana e machine learning, Darktrace crea un profilo comportamentale unico per ciascun utente e dispositivo all'interno dell'ambiente di rete. Inoltre, è in grado di raggruppare gli utenti e i dispositivi in base ai loro comportamenti, consentendo così di rilevare anomalie nel caso in cui un utente o un dispositivo si discosti dal comportamento tipico del suo gruppo.

Operando in tempo reale e analizzando il traffico di rete in modo continuo, Darktrace è in grado di identificare anche gli attacchi "zero-day", che non seguono schemi precedentemente noti. Per garantire l'affidabilità delle segnalazioni, Darktrace utilizza un'intelligente soglia di rilevamento che contestualizza e aggiorna costantemente le segnalazioni in base alle rilevazioni precedenti, riducendo al minimo i falsi positivi e mitigando il rischio di distorsioni dovute al tasso di base.
Darktrace è composto da quattro moduli distinti: Darktrace PREVENT, Darktrace DETECT, Darktrace RESPOND e Darktrace HEAL. Tuttavia, durante il tirocinio, ci concentreremo esclusivamente sui moduli DETECT e RESPOND, in quanto sono gli unici utilizzati durante l'esperienza pratica[23].

2.2.4 Darktrace DETECT

Darktrace DETECT offre un'interfaccia che segnala le anomalie e fornisce gli strumenti per valutare se sono comportamenti legittimi nell'ambiente lavorativo o malevoli. Le violazioni dei modelli possono essere parte di un incidente dell'AI Analyst o un'allerta autonoma, comunicando agli utenti tramite l'interfaccia Threat Visualizer comportamenti anomali di dispositivi o account[24].
Un modello è composto da tre elementi fondamentali:

- Condizioni del modello: sono componenti che, quando soddisfatte, provocano una violazione del modello. Ogni componente è composto da una metrica con le proprie condizioni filtro, come l'utilizzo di protocolli specifici o pacchetti HTTP con User Agent rari. Questi elementi, insieme, costituiscono la logica del modello.

- Modulazione del punteggio: comprende quattro modelli che influenzano il comportamento del modello quando viene attivato. Il modello standard specifica che una continua violazione nel tempo diminuisce il punteggio, ma esistono anche altre modalità: una modulazione che mantiene lo stesso punteggio nel tempo e un'altra che aumenta il punteggio dopo le prime violazioni e poi lo diminuisce.

- Azioni del modello: sono azioni di sistema che possono essere attivate in risposta a una violazione del modello. Queste azioni possono includere l'invio di email o notifiche HTTP. Inoltre, è possibile selezionare una criticità diversa da quella standard o segnalare la violazione come "Informational"[25].

Solo una parte degli incidenti viene segnalata dall'*AI Analyst* di Darktrace, il quale raccoglie molteplici informazioni rilevanti e le presenta in un formato facilmente comprensibile per l'operatore. Questo strumento investiga, analizza e categorizza le minacce all'interno dell'ambiente, identificando incidenti potenzialmente interessanti e insoliti, spesso raggruppandoli per un singolo dispositivo. Gli incidenti che coinvolgono più dispositivi sono classificati come incidenti "*cross-network*". L'*AI Analyst* non si limita a investigazioni autonome e non sollecitate, ma è anche disponibile su richiesta per un dispositivo selezionato da parte dell'operatore.
Per quanto riguarda le allerte autonome, è compito dell'analista indagare su di esse utilizzando gli strumenti forniti da Darktrace DETECT per rispondere alle 5 W:

1. Who?: identificare chi ha scatenato l'allarme.

2. What?: comprendere quale azione è stata compiuta.

3. When?: determinare quando sono avvenute tali operazioni.

4. Where?: individuare il dispositivo o il luogo in cui sono state effettuate tali operazioni.

5. Why?: capire il motivo per cui Darktrace ha segnalato questa anomalia.

Se la legittimità dell'attività non è immediatamente chiara attraverso le informazioni fornite dalla violazione del modello, è consigliabile contattare l'utente finale, poiché la consultazione e la collaborazione con gli utenti sono fondamentali per una valutazione completa della situazione[24].

2.2.5 Darktrace RESPOND

Darktrace RESPOND/Network è progettato per gestire minacce di sicurezza di alto livello, come ad esempio i ransomware. Utilizzando due approcci distinti, può interrompere le connessioni malevole sia attraverso il reset TCP che integrandosi direttamente con il firewall esistente, inviando messaggi direttamente a esso.
Il flag RST del protocollo TCP è una componente delle comunicazioni standard tra dispositivi: quando un endpoint riceve un pacchetto con questo flag attivato, la connessione viene immediatamente interrotta. Darktrace rileva attività sospette e, in caso di anomalie, invia pacchetti di reset TCP a entrambi i dispositivi coinvolti, sia all'interno che all'esterno della rete, per interrompere la connessione malevola. Gli indirizzi IP dei pacchetti di reset sono falsificati per far credere ai dispositivi che non provengano da Darktrace, ma l'uno dall'altro.
Darktrace RESPOND può attuare una serie di azioni proattive, misurate e automatizzate in risposta a minacce informatiche confermate rilevate in tempo reale. I componenti di Darktrace RESPOND possono essere utilizzati in due modalità distinte:

- **Modalità di conferma umana**: le azioni di Darktrace RESPOND rimarranno in sospeso fino a quando un operatore umano non conferma o ignora la segnalazione del modulo RESPOND.

- **Modalità autonoma o parzialmente autonoma**: in modalità completamente autonoma, RESPOND risponde automaticamente alle minacce, mentre nella modalità parzialmente autonoma, può essere attivato autonomamente al di fuori degli orari lavorativi, ma richiede conferma umana per il resto del tempo.

Darktrace RESPOND reagisce alle violazioni dei modelli offrendo l'opzione di impostare un inibitore, che è un'azione finalizzata a contrastare il comportamento anomalo del dispositivo o dell'utente. Gli inibitori disponibili includono:

- **Bloccare le connessioni corrispondenti**: interrompe le connessioni dal dispositivo all'endpoint di destinazione identificato nell'incidente, sulla porta di destinazione osservata.

- **Imporre il pattern di vita**: consente al dispositivo di effettuare solo connessioni e trasferimenti di dati considerati normali da Darktrace, basati sui modelli di vita definiti per quel dispositivo. Qualsiasi attività che si discosti da questi modelli viene bloccata.

- **Imporre il pattern di vita del gruppo**: permette al dispositivo di intraprendere le stesse connessioni e trasferimenti di dati che sono comuni tra i dispositivi nel suo gruppo di pari, basandosi sui modelli di vita del gruppo.
- **Quarantena del dispositivo**: blocca tutto il traffico di rete in entrata e in uscita dal dispositivo, isolandolo dalla rete.
- **Blocco di tutti i traffici in uscita**.
- **Blocco di tutti i traffici in entrata**[26].

Capitolo 3

Sperimentazione con Tpot e Darktrace

In sezione 3.1, viene illustrata l'implementazione di T-Pot, inclusa l'installazione e la configurazione iniziale (3.1.1), l'implementazione degli script e degli automatismi necessari per il suo funzionamento (3.1.2), e una panoramica sui dati raccolti durante i test (3.1.3).
Nella sezione 3.2, vengono esaminate le minacce rilevanti dal punto di vista pratico, sia quelle importanti (3.2.1) che quelle quotidiane (3.2.2).
Infine, la sezione 3.3 fornisce un riassunto dei vantaggi che possono derivare dall'integrazione di entrambi i sistemi.

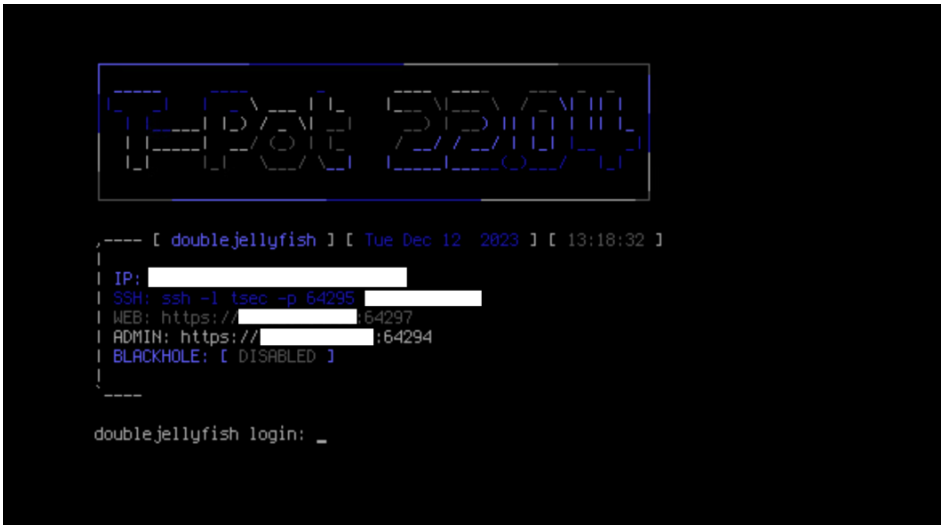
3.1 Implementazione di Tpot e analisi dei risultati

3.1.1 Configurazione di base

Per prima cosa, è fondamentale verificare di avere tutti i prerequisiti necessari per l'installazione corretta dell'honeypot, questi prerequisiti sono: un indirizzo IP fornito da un server DHCP e una connessione ad Internet, spazio di archiviazione minimo necessario, spazio di memoria RAM. Queste ultime due possono variare in base alla tipologia di installazione *standalone* o *distribuita*. Successivamente, dalla pagina ufficiale Github di T-Pot deve essere scaricata l'immagine ISO; si tratta di un file che contiene l'immagine del sistema operativo preconfigurato con tutti gli strumenti e le funzioni necessarie per T-Pot. Una volta scaricata l'immagine ISO, il passo successivo è l'installazione effettiva dell'immagine. Ciò deve avvenire seguendo attentamente i passaggi indicati fino al completamento dell'installazione, potendo scegliere quale dei tre tipi installare:

- *Standalone*: è la versione completa in cui vengono installati tutti i sistemi per far si che funzioni autonomamente.
- *Sensor*: è la versione che installa solo il sensore, quindi comprende solo gli honeypot e non i pacchetti per la gestione via interfaccia web.
- *Hive*: versione che non include honeypot ma solo programmi per il collegamento ed il controllo da remoto in quanto adibita a raccogliere i dati dalle versioni *sensor*, grazie all'uso di tunnel SSH.

Una volta completata l'installazione, viene visualizzato un prompt contenente le informazioni per connettersi al sistema da remoto, questo può essere effettuato tramite l'interfaccia web contenente un terminale oppure tramite connessione SSH. La seguente immagine viene visualizzata in caso T-Pot sia stato installato correttamente ed è pronto all'uso.



Dopo aver completato l'installazione di T-Pot, è necessario apportare alcune modifiche e configurazioni aggiuntive per assicurarsi che funzioni correttamente.
Il primo passaggio dopo l'installazione è modificare il file */etc/network/interface* per configurare correttamente l'interfaccia di rete primaria dell'honeypot. Dopo aver apportato le modifiche al file di configurazione, è necessario riavviare l'interfaccia di rete affinché le modifiche abbiano effetto. Successivamente, è importante installare e configurare il server di posta Postfix utilizzando il gestore di pacchetti apt. Postfix è necessario per consentire a T-Pot di inviare mail contenenti le segnalazioni di connessioni malevole.
Durante la configurazione di Postfix, è essenziale assicurarsi che sia configurato per utilizzare la porta 587 per le comunicazioni email anziché la porta standard 25. Ciò è particolarmente importante perché la porta 25 viene occupata dagli Mailoney, mentre la porta 587 offre una maggiore sicurezza.

3.1.2 Script e automazioni

Lo scopo del progetto era di inviare dati degli attacchi subiti da T-Pot al SIEM tramite plugin o programmi esistenti, ma poiché non erano disponibili soluzioni adatte alle esigenze aziendali, è stato sviluppato uno script per analizzare i log dei principali honeypot:

- Dionaea: utilizzato per monitorare la porta legata al protocollo FTP(21).
- Cowrie: utilizzato per monitorare le porte legate ai protocolli SSH e Telnet(22, 23).
- Tanner: utilizzato per monitorare le porte legate al protocollo HTTP(80, 8080).

- Citrixhoneypot: utilizzato per monitorare le porte legate al protocollo HTTPS(443).
- Honeytrap: utilizzato per monitorare un gruppo di porte non standard, le porte maggiori di 1024.

Lo script estrae le informazioni rilevanti dai log di ogni honeypot e le formatta per l'integrazione con il SIEM.

Listing 3.1: CEF_Script.sh

```
#!/bin/bash

honeytrapFile="/data/honeytrap/log/attacker.log"

honeytrapBackup="/home/tsec/script/backup/honeytrap/backup.log"

messaggio=""

if [ ! -e "$honeytrapBackup" ]; then
touch $honeytrapBackup
fi

diffHoneytrap=$(diff $honeytrapFile $honeytrapBackup)
if [ "$diffHoneytrap" != "" ]; then
tmpHoneytrap="/tmp/diffHoneytrap"
diff $honeytrapFile $honeytrapBackup | grep -E '^<|^>' | sed 's/^< //'
    ↪ > $tmpHoneytrap
cp $honeytrapFile $honeytrapBackup
chown tsec:tsec $honeytrapBackup
honeytrapAttaccoPort=$(awk -F'[: ]+' '/^.*tcp/ { print "DeviceName=
    ↪ Honeypot DestinationIP="$11" DestinationPort="$12"
    ↪ ApplicationProtocol= SourceIP="$8" SourcePort="$9"" }'
    ↪ $tmpHoneytrap | sort -u)
if [ ! -z "$honeytrapAttaccoPort" ]; then
messaggio+="Sono state riscontrate le seguenti connessioni alle porte
    ↪ dell'honeypot:\n$honeytrapAttaccoPort\n"
messaggioCEF=$(awk -F'[: ]+' '/^.*tcp/ { print $12" "$8 }'
    ↪ $tmpHoneytrap | sort | uniq -c | awk '{print "reason=Honeytrap
    ↪ cn1="$1" src="$3" dpt="$2}')

echo "$messaggioCEF" | while IFS= read -r linea; do
if [ ! -z "$linea" ]; then
logger -p local4.warn -P 514 -n 127.0.0.1 --rfc3164 -t CEF "0|Honeypot-
    ↪ Test|Honeypot-Test|0.1|event-honeypot-test|end|TRAFFIC|$linea"
fi
done
fi
rm -f $tmpHoneytrap
```

```
fi

if [ ! -z "$messaggio" ]; then
echo -e "To: provaAlertEmailMatteo@gmail.com\nSubject: Connessioni all'
    ↪ honeypot\n$messaggio" >> /tmp/mailTemp.txt
/usr/sbin/sendmail provaAlertEmailMatteo@gmail.com < /tmp/mailTemp.txt
rm -f /tmp/mailTemp.txt
fi
```

Ecco una spiegazione delle principali azioni svolte dallo script:

1. Viene definito il percorso del file di log dell'honeypot e il percorso del file di backup che conterrà una copia del file di log per confronti successivi.
2. Se il file di backup non esiste, viene creato.
3. Viene eseguito un confronto tra il file di log attuale e quello di backup per individuare eventuali differenze.
4. Se vengono rilevate delle differenze, vengono estratte le informazioni sulle connessioni di attacco dal file di log attuale.
5. Queste informazioni vengono aggiunte a un messaggio di notifica che sarà inviato tramite email.
6. Viene generato un messaggio nel formato CEF (Common Event Format) per ciascuna connessione di attacco trovata.
7. Infine, se è stato creato un messaggio di notifica, viene creato un file temporaneo contenente il testo dell'email di notifica e viene inviata l'email utilizzando il comando sendmail.

Questo processo viene effettuato per i cinque honeypot elencati precedentemente. Per far sì che lo script esegua il controllo dei log ogni minuto, è necessario configurare il file crontab. Questo file è collegato al comando crontab, il quale, all'avvio del sistema, esegue un demone che legge il file ogni minuto.
Successivamente, è necessario creare un altro script che permetta la cancellazione delle cartelle di backup utilizzate per il confronto all'avvio del sistema, al fine di mantenere la logica del programma integra.

Listing 3.2: Delete_Script.sh

```
#!/bin/bash

# Specifica i percorsi dei file che vuoi cancellare
dionaeaBackup="/home/tsec/script/backup/dionaea/backup.json"
cowrieBackup="/home/tsec/script/backup/cowrie/backup.json"
tannerBackup="/home/tsec/script/backup/tanner/backup.json"
citrixhoneypotBackup="/home/tsec/script/backup/citrixhoneypot/backup.
   ↪ log"
honeytrapBackup="/home/tsec/script/backup/honeytrap/backup.log"

# Cancella i file
rm -f $dionaeaBackup $cowrieBackup $tannerBackup
rm -f $citrixhoneypotBackup $honeytrapBackup

# Aggiungi altre operazioni di pulizia, se necessario
echo "File cancellati con successo."
```

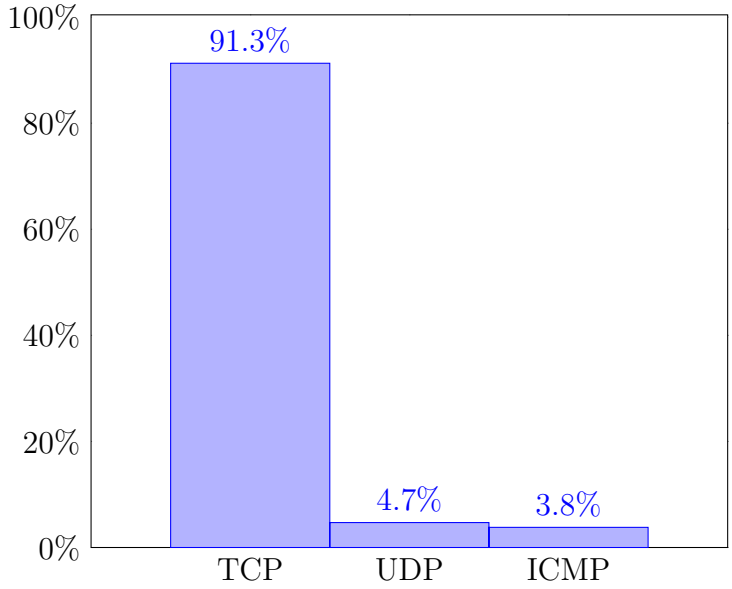
Una volta creato quest'ultimo script, è necessario creare un servizio che esegua quest'ultimo script ad ogni avvio della macchina. Questo può essere fatto utilizzando i servizi di systemctl con il seguente codice:

Listing 3.3: Delete_Backup.service

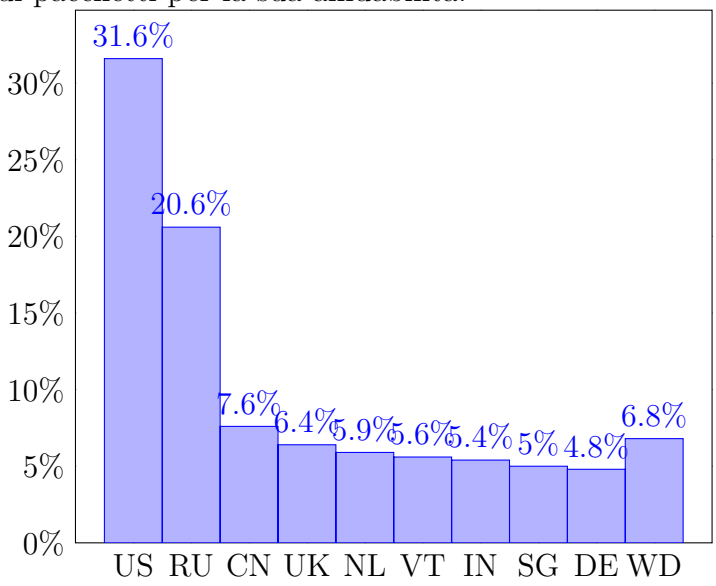
```
[Unit]
Description=Script per cancellare file prima del riavvio

[Service]
Type=oneshot
ExecStart=/usr/local/bin/delete_backup.sh

[Install]
WantedBy=multi-user.target
```

3.1.3 Dati raccolti

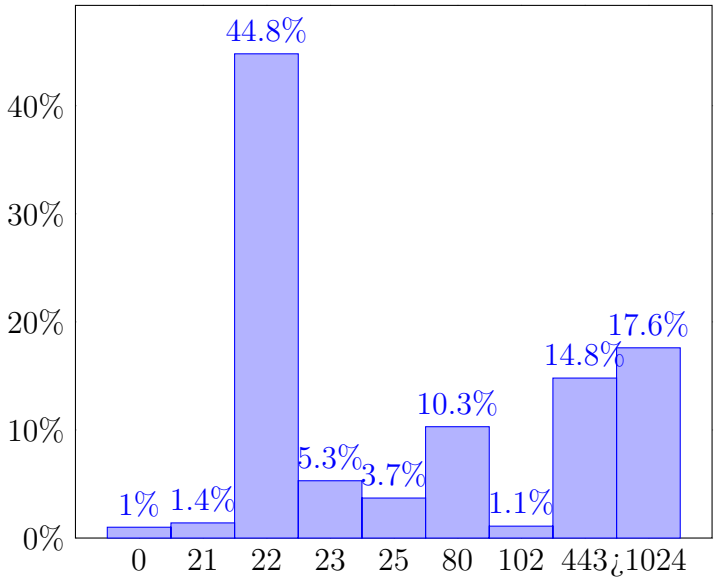
I dati qui mostrati riguardano tutti gli attacchi subiti dall'honeypot, non solo quelli raccolti dallo script, nell'arco temporale di una settimana in cui T-Pot è stato esposto a Internet.



L'analisi dei dati raccolti rivela che la quasi totalità dei pacchetti ricevuti è di tipo TCP, rappresentando il 91,3% del totale, seguito da UDP con il 4,7% e ICMP con il 3,8%. Questo è in linea con il fatto che il protocollo TCP richiede un maggior numero di pacchetti per la sua affidabilità.



Mentre dal punto di vista geografico, gli Stati Uniti d'America, la Russia e la Repubblica Popolare Cinese sono i principali attori; infatti, contribuiscono complessivamente al 59,8% di tutti gli attacchi registrati, seguiti da altri paesi come Regno Uniti, Paesi Bassi, Vietnam, India, Singapore, Germania e il resto del mondo, che rappresenta il 6,8%.



Nel dettaglio delle porte più attaccate, la porta 22 (SSH) risulta essere quella bersagliata più frequentemente, il 44,8% di tutti gli attacchi diretti sono a questa porta. Le porte 443 (HTTPS) e 80 (HTTP) seguono rispettivamente con il 14,8% e il 10,3%. Altre porte di rilevanza includono la porta 23 (Telnet) e la porta 25 (SMTP), mentre le porte non standard, quelle non standard (>1024), contribuiscono in misura minore agli attacchi subiti.

3.2 Monitoraggio delle reti con Darktrace

3.2.1 Minacce importanti rilevate

Nel contesto di questa sezione, saranno esaminati tre casi di anomalie rilevate e risolte utilizzando Darktrace.
Il primo caso riguarda il worm Conficker (CVE-2008-4250), scoperto nel 2008, che sfrutta una vulnerabilità non ancora corretta di Microsoft Windows, al fine di violare la password di amministratore locale. Una volta ottenuto il controllo di un dispositivo, il worm cerca di diffondersi ad altre macchine nella rete. Darktrace ha riconosciuto questa minaccia tramite il rilevamento di grandi richieste DNS domini generati da algoritmi (DGA). Di fronte a tale minaccia, Darktrace ha messo automaticamente il dispositivo interessato in quarantena, rimuovendolo dalla rete fino a quando un operatore umano non ha deciso di rilasciarlo.
La seconda anomalia significativa coinvolge l'uso di strumenti di attacco e ricognizione, come Nmap, Nessus o OpenVAS, da parte di un dispositivo di rete per condurre scansioni e catalogare informazioni su indirizzi IP, porte aperte, sistemi operativi e vulnerabilità. Darktrace ha riconosciuto quante e quali porte/servizi sono stati scansionati ed è intervenuto bloccando tutte le connessioni in uscita del dispositivo coinvolto. L'analista responsabile ha poi contattato il cliente per informarlo sull'attività sospetta all'interno della sua rete.
Infine, nel terzo caso, Darktrace ha rilevato un'anomalia denominata "Ransomware / SMB Reads then Writes with Additional Extensions". In questo scenario, è stato osservato un dispositivo che ha letto un gran numero di file SMB con un'estensione specifica, seguito dalla scrittura di un numero corrispondente di file con un'estensione aggiuntiva.

Questo comportamento poteva essere indicativo di un attacco ransomware. Darktrace ha consigliato di esaminare attentamente i file scritti per verificare se corrispondessero a un'estensione tipica dei ransomware.

3.2.2 Esempi di segnalazioni quotidiane

Le segnalazioni quotidiane possono essere suddivise in due categorie: comune e media gravità. Tra gli incidenti comuni segnalati quotidianamente troviamo:

- `Plaintext password`: questo tipo di segnalazione indica l'individuazione di login inviati in chiaro, ovvero senza alcuna cifratura delle credenziali. Questi eventi possono verificarsi nei protocolli HTTP o LDAP. I login scoperti vengono successivamente inclusi nel report settimanale inviato all'azienda.

- `Possible Unencrypted Password File On Server`: questo incidente si verifica quando un dispositivo apre un documento con nel titolo le parole "password", "pwd" o "secret", e non utilizza un formato noto per la sicurezza, ma un formato comune come .doc o .xlsx. Tali file vengono segnalati nel report settimanale.

- `Anonymous NTLM logins`: questa segnalazione avviene quando un dispositivo tenta di autenticarsi con altri dispositivi tramite NTLM utilizzando un account utente anonimo. Questi tentativi di login anonimi vengono poi inclusi nel report settimanale consegnato al cliente.

Le segnalazioni di media gravità, che richiedono un'analisi più approfondita, includono:

- `Suspicious Domain`: questo tipo di segnalazione avviene quando un dispositivo si connette a un dominio esterno raro, non comunemente visitato all'interno della rete, con un dominio di primo livello (TLD) associato ad attività dannose, come ad esempio "example.top". Il compito dell'analista è verificare la legittimità del sito, utilizzando strumenti come Cisco Talos o VirusTotal.

- `Unusual Admin RDP Session`: questa segnalazione si verifica quando viene effettuata una connessione RDP (Remote Desktop Protocol) con credenziali di amministratore. L'analista contatta solitamente il cliente per verificare la legittimità dell'operazione.

- `BitTorrent`: viene segnalato quando un dispositivo stabilisce connessioni peer-to-peer BitTorrent, spesso associato alla condivisione di dati protetti da copyright o ad altre informazioni indesiderate. In questo caso, si consiglia al cliente di indagare sulla quantità di dati scaricati e di disinstallare il programma dai dispositivi aziendali.

3.3 Integrare Darktrace e Tpot per una maggiore sicurezza

L'integrazione di Darktrace e T-Pot offre una serie di vantaggi significativi per la sicurezza informatica. Da un lato, Darktrace con la sua capacità di rilevare e prevenire

intrusioni in tempo reale, consente di identificare e rispondere prontamente alle minacce attive. Tuttavia, può essere limitato dalla sua capacità di rilevare solo le minacce già note o le firme di attacco conosciute. D'altro, T-Pot agisce come esca per attirare gli attaccanti e raccogliere informazioni sulle loro tattiche e strategie. Integrando questi due strumenti, è possibile prevenire gli attacchi esterni, i quali vengono attratti e intrappolati da T-Pot; contemporaneamente è possibile bloccare gli attacchi che si verificano all'interno della rete, migliorando così complessivamente la sicurezza dell'ambiente informatico.

Capitolo 4

Conclusioni

Il lavoro illustrato in questa tesi ha segnato un importante traguardo nell'ambito della sicurezza informatica aziendale, attraverso l'efficace implementazione di un honeypot e la gestione di un IDPS. L'adozione di un progetto open-source predefinito ha agevolato il percorso, permettendo di dedicare maggiori risorse all'espansione e al potenziamento dei servizi offerti. Sebbene ciò abbia semplificato la fase iniziale di installazione, l'integrazione con il SIEM ha richiesto un impegno sia di tempo che di studio aggiuntivo, evidenziando l'importanza di una profonda comprensione del contesto aziendale e dei suoi requisiti specifici.
Il percorso seguito, partendo dalla fase preliminare di studio e definizione degli obiettivi, attraverso la fase di progettazione e l'effettiva implementazione del progetto, ha dimostrato di essere un metodo efficace nel conseguimento degli obiettivi prefissati. L'honeypot sviluppato è risultato efficace nel mitigare il traffico dannoso proveniente dagli attaccanti, mentre le competenze acquisite nell'utilizzo di Darktrace hanno notevolmente arricchito le capacità difensive aziendali.
Per quanto riguarda i futuri sviluppi, il prossimo passo potrebbe essere quello di valutare l'offerta del servizio ai clienti, qualora vengano riscontrati benefici a lungo termine, da affiancare al monitoraggio già fornito dal SOC tramite Darktrace. In tal senso, potrebbe essere considerata l'installazione delle distribuzioni sensore di T-pot all'interno delle subnet utilizzate dai clienti. Queste distribuzioni sarebbero in grado di rilevare e bloccare qualsiasi attività sospetta tramite il SIEM, offrendo così un livello aggiuntivo di protezione.
Al fine di agevolare l'adozione di questa soluzione da parte dei clienti, è stata redatta una documentazione esaustiva, finalizzata a semplificare l'implementazione e l'utilizzo della piattaforma, garantendo che i vantaggi e le potenzialità dell'honeypot e dell'IDPS possano essere pienamente sfruttati. La ricerca continua di miglioramenti e l'adattamento alle esigenze emergenti del panorama della sicurezza informatica rimarranno al centro delle future attività, con l'obiettivo primario di garantire una protezione sempre più efficace contro le minacce in continua evoluzione.

Capitolo 5

Bibliografia

[1] R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949. National Institute of Standards e Technology, 2007.

[2] Lance Spitzner. *Honeypots: Tracking Hackers*. 2002.

[3] Clifford Stoll. *The Cuckoo's Egg*. Doubleday, 1989.

[4] William Cheswick. "An Evening with BerferdIn Which a Cracker is Lured, Endured, and Studied". In: *cheswik.com* (1991).

[5] "The word for bear". In: *University of Pittsburg Journal* (2014).

[6] Michele Adams Iyatiti Mokube. *Honeypots: Concepts, Approaches, and Challenges*. Article. Armstrong Atlantic State University, 2007.

[7] Michele Adams Iyatiti Mokube. *Honeypots: Concepts, approaches, and challenges*. ACM-SE 45, 2007, pp. 321–326.

[8] Lance Spitzner. *Honeypots tracking hackers*. Addison-Wesley, 2007, pp. 68–70.

[9] Nile Provos. *A Virtual Honeypot Framework*. Rapp. tecn. Google, Inc., 2010.

[10] David Tidmarsh. "What Is a Honeypot in Cybersecurity? Types, Implementation, and Real-World Applications". In: *EC-Council* (2023).

[11] Mark Joseph Edwards. "Antispam Honeypots Give Spammers Headaches". In: *Windows IT Pro* (2002).

[12] "Secure Your Database Using Honeypot Architecture". In: *DBCoreTech* (2010).

[13] Hsinchun Chen Arthur Jicha Mark Patton. "SCADA honeypots: An in-depth analysis of Conpot". In: *IEEE* (2013).

[14] Peter Mell Rebecca Brace. *Intrusion Detection Systems*. NIST Special Pubblication 800-31. National Institute of Standards e Technology, 2001.

[15] James Anderson. "Computer Security Threat Monitoring and Surveillance". In: *NIST* (1980).

[16] Dorothy Elizabeth Denning. *An Intrusion Detection Model*. Proceedings of the Seventh IEEE Symposium on Security e Privacy, 1986, pp. 119–131.

[17] Theresa F. Lunt. "IDES: An Intelligent System for Detecting Intruders". In: *Proceedings of the Symposium on Computer Security; Threats, and Countermeasures* (1990), pp. 110–121.

[18] Stefan Axelsson. *Intrusion Detection Systems: A Survey and Taxonomy*. Rapp. tecn. Department of Computer Engineering Chalmers University of Technology Göteborg, Sweden, 2000.

[19] John R. Vacca. *Network and system security*. 2013.

[20] Peter Mell Karen Scarfone. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. Rapp. tecn. National Institute of Standards e Technology, 2010.

[21] Dimitrios N. Serpanos Christos Douligeris. *Network Security: Current Status and Future Directions*. John Wiley e Sons, 2007.

[22] Hagar S Elsayed Rowayda A. Sadek M Sami Soliman. *Effective anomaly intrusion detection system based on neural network with indicator variable and rough set reduction*. Rapp. tecn. International Journal of Computer Science Issues, 2013.

[23] Darktrace Limited Holding. *Threat Visualizer part 1 - Familiarization*. `https://customerportal.darktrace.com`. 2023.

[24] Darktrace Limited Holding. *Threat Visualizer part 2 - Investigation*. `https://customerportal.darktrace.com`. 2023.

[25] Darktrace Limited Holding. *Cyber Analyst Part 2 - Model Optimizationn*. `https://customerportal.darktrace.com`. 2023.

[26] Darktrace Limited Holding. *Darktrace RESPOND/Network*. `https://customerportal.darktrace.com`. 2023.