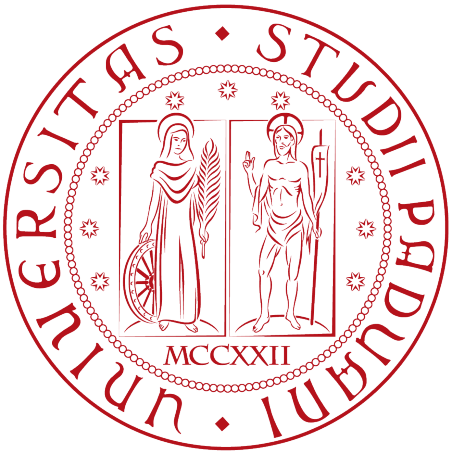
Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea in Informatica



Progettazione e implementazione di un sistema di Network Detection and Response

Tesi di laurea

Relatore interno

Prof. Claudio Enrico Palazzi

Relatore aziendale

Roberto Pezzile

Laureando

Elia Pasquali

Matricola 1225412

Anno Accademico 2023-2024

Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage, della durata di circa trecentoventi ore, dal laureando Elia Pasquali presso l'azienda Wintech S.p.A nel periodo che va dal 05/06/2023 al 02/08/2022, con il supporto del tutor aziendale Roberto Pezzile, del collega Mirco Cailotto, e del relatore interno all'Università Prof. Claudio Enrico Palazzi.

Lo scopo di questo stage riguardava la progettazione e l'implementazione di un sistema di *Network Detection and Response* in un contesto reale e complesso come un'infrastruttura aziendale, descrivendo gli obiettivi raggiunti e le problematiche incontrate e, nel caso, risolte.

In questo documento viene descritta l'organizzazione del suddetto stage, le tecnologie studiate e utilizzate, il prodotto su cui si è lavorato e le attività svolte. Al termine verranno raccolte delle conclusioni personali sul lavoro svolto e sulle conoscenze acquisite.

Ringraziamenti

Desidero ringraziare la mia famiglia che mi ha sempre supportato in ogni mia scelta e che mi ha permesso di arrivare fino a qui.

Ringrazio Roberto, Mirco, Andrea, Romano, Denis e tutti gli altri in Wintech che mi hanno aiutato durante il mio percorso di stage.

Ringrazio il Prof. Claudio Enrico Palazzi, relatore della mia tesi, per avermi seguito in questo progetto.

Ringrazio tutti gli amici, da quelli storici alle nuove conoscenze fatte in questi anni, con cui ho condiviso varie avventure e che mi hanno spinto a dare il massimo.

Arcole, Settembre 2023 Elia Pasquali

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione

1.1 L'azienda

Winning Technology S.p.A è un'azienda nata nel 1987 da un'idea del suo fondatore e attuale amministratore delegato Massimo Gallotta. Wintech è un *System Integrator* che opera nel settore *Information and Communication Technology*, spesso abbreviato in ICT, che raggruppa tutti i servizi legati allo sviluppo di soluzioni software, hardware e progettazione ad hoc legati all'informatica e alle telecomunicazioni.

L'azienda ha sede principale a Padova ed è arrivata ad espandersi in altre tre sedi, una a Milano, una a Bassano del Grappa e l'ultima a Pordenone, contando più di 90 risorse divise tra le varie filiali.[1]

Figura 1.1: Logo di Wintech S.p.A.

1.2 L'idea

Lo scopo dello stage è quello di fornire una formazione approfondita sulle tecnologie e le metodologie relative agli strumenti di *Network Detection and Response* (NDR). In particolare, lo studente avrà l'opportunità di acquisire competenze specialistiche sulla progettazione, l'implementazione e la gestione di un sistema di NDR scelto dall'azienda che verrà inserito all'interno della propria infrastruttura.

Un sistema di NDR è uno strumento che consente di individuare rapidamente i pericoli nella rete e di attuare una *remediation* automatica. Monitora costantemente il traffico di rete e analizza i dati raccolti, per identificare eventuali attività sospette o pericolose. In caso di pericolo, il sistema può attivare una risposta automatica o notificare un amministratore di sistema, consentendo di rispondere in modo rapido ed efficace a potenziali attacchi.

Durante lo stage, il candidato ha lavorato alla progettazione e all'implementazione del sistema, configurando i dispositivi di sicurezza della rete, definendo le regole e le

politiche di sicurezza, per poi verificarle simulando degli attacchi e analizzare i dati di monitoraggio per identificare eventuali attività sospette. L'obiettivo finale del progetto è stato quello di mettere in produzione il sistema al termine dello stage, in un contesto complesso e articolato di tre *data center* collegati in rete geografica nazionale.

1.3 Organizzazione del testo

Il secondo capitolo descrive il contesto aziendale e il suo approccio nei vari ambiti lavorativi

Il terzo capitolo descrive in dettaglio il progetto di stage e la sua pianificazione

Il quarto capitolo raccoglie tutto ciò che è stato studiato per comprendere il contesto applicativo e le varie tecnologie utilizzate

Il quinto capitolo approfondisce il prodotto e le funzionalità che offre

Il sesto capitolo descrive le attività svolte durante lo stage

Il settimo capitolo raccoglie i risultati ottenuti e alcune considerazioni personali

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

- I termini tecnici e in lingua straniera sono scritti in *corsivo*, mentre pezzi di codice invece verranno scritti in carattere `monospaziato`;
- Le figure e le tabelle possiedono una descrizione e una numerazione progressiva legata al capitolo di appartenenza.

Data la natura del progetto, sono stati raccolti e analizzati dati riservati aziendali e dei clienti, per questo motivo, dalle immagini sono state rimosse tutte le componenti che potrebbero rivelare informazioni sensibili.

Per alleggerire il documento, sono stati inserite delle appendici che contengono informazioni aggiuntive e approfondimenti su alcuni argomenti trattati, come ad esempio la configurazione di alcuni dispositivi di rete in Appendice A e alcuni attacchi e mitigazioni in Appendice B.

Capitolo 2

Contesto aziendale

In questo capitolo viene descritto il contesto in cui l'azienda opera e come essa si approccia ai propri progetti.

2.1 Prodotti e servizi

L'azienda si occupa di fornire servizi di consulenza, progettazione e sviluppo di soluzioni software e hardware, oltre a fornire servizi di *outsourcing* dell'infrastruttura. Tra i clienti di Wintech possiamo trovare professionisti, PMI e grandi aziende, banche, assicurazioni e pubblica amministrazione.

I prodotti principali e più richiesti sono software per la gestione documentale e l'ottimizzazione dei processi aziendali, programmi *ERP* e di *Business Intelligence*, fino ad arrivare a consulenze personalizzate per soluzioni *IT*, di *CyberSecurity* e *design* di *intranet* aziendali.

2.1.1 Cloud

Wintech offre servizi *cloud* mirati alle aziende e certificati secondo lo standard ISO 27001. Per un cliente, questo si traduce nela possibilità di accedere a potenti risorse informatiche, affidabili e scalabili, senza dover effettuare grandi investimenti in una infrastruttura interna, con relativi costi di creazione, gestione e formazione dei dipendenti. Affidandosi quindi ad un fornitore con esperienza si può lavorare con la sicurezza di avere le ultime tecnologie senza doversi preoccupare dei rischi.[2]

L'infrastruttura offerta da Wintech sfrutta strumenti all'avanguardia e si affida a partner nazionali di rilievo come *VSIX* e *DATA4* e internazionali quali *Microsoft Azure* e *Amazon AWS* (Figura 2.1)

2.1.2 Security

Negli ultimi anni l'ambito della sicurezza informatica per le aziende sta diventando sempre più di rilievo e di fondamentale importanza. Wintech si mantiene aggiornata in questo settore estremamente dinamico, dove ogni giorno vengono scoperte nuove falle e vulnerabilità, che devono essere tempestivamente risolte.

L'approccio di Wintech è quello di fornire soluzioni di sicurezza che siano in grado di proteggere i dati e le informazioni aziendali, definendo vari livelli di sicurezza per ogni tipo di risorsa. Tutte le soluzioni proposte dall'azienda sono costruite in modo

(a) Logo di VSIX

(b) Logo di DATA4

(c) Logo di Microsoft Azure

(d) Logo di Amazon AWS

Figura 2.1: Loghi partner cloud di Wintech

da essere conformi al *GDPR*, senza demonizzarlo, ma anzi andando a sfruttare le opportunità che esso offre per migliorare la sicurezza e la consapevolezza dei clienti.

In Figura 2.2 viene mostrato come l'azienda si dedica ai propri progetti, proponendo soluzioni e framework maturati nel tempo e in continuo aggiornamento per rimanere all'avanguardia e sostenibili. Come viene citato nel sito aziendale:

> «La **Sicurezza** deve essere intesa come un processo aziendale cross a tutti gli altri, volto a valutare costantemente integrità delle informazioni, garantire corretta riservatezza e puntuale visibilità dei dati mantenendo disponibilità e accessibilità secondo esigenze di continuità richieste dal business o servizio specifico.» [3]

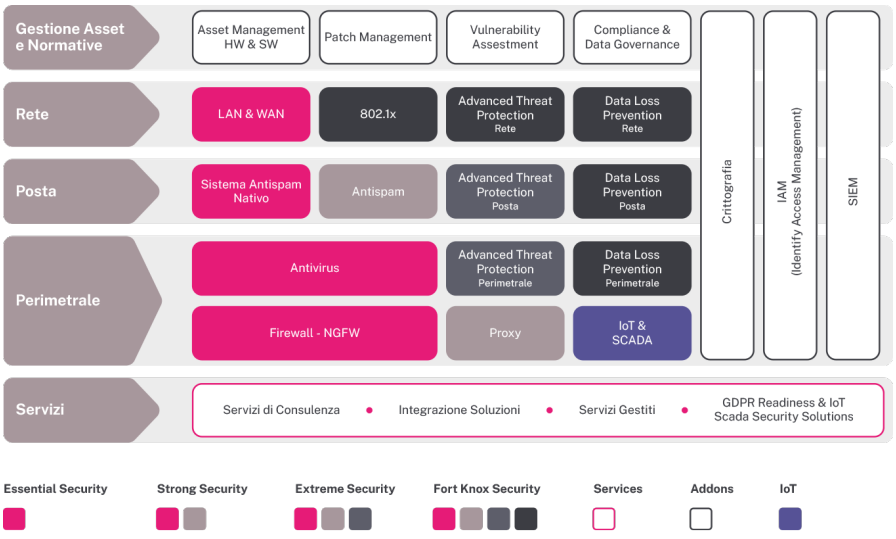


Figura 2.2: Matrice della Sicurezza in Wintech

2.2 Partnership e Certificazioni

Come supporto a tutto il proprio lavoro, Wintech ha dalla sua parte una serie di *partnership* con produttori e fornitori degli strumenti che poi utilizza. Tra questi troviamo aziende come *HPE Aruba*, *Cambium Networks*, *PaloAlto Networks* e *Watchguard* per il lato *network* e altre come *Nutanix*, *Veeam* e *WMware* per la parte di infrastruttura e virtualizzazione.[1] Inoltre mantiene un rapporto abbastanza diretto tra se e le aziende con cui collabora come *Grandstream* e *Sangfor*, la seconda oggetto del mio progetto di stage.

Figura 2.3: Loghi dei partner di Wintech

Dal lato delle certificazioni invece, l'azienda è certificata rispetto agli standard **UNI CEI ISO/IEC 9001:2015** e **UNI CEI ISO/IEC 27001:2017**. La prima attesta la qualità per le attività di progettazione, implementazione e fornitura di sistemi informativi integrati, progettazione e sviluppo di soluzioni software e erogazione di assistenza tecnica, sistematica e applicativa.

La seconda invece assicura che i servizi sistemistici e di *network* forniti in *outsourcing* garantiscano **riservatezza** rispetto agli accessi alle informazioni e **integrità** e **disponibilità** di queste ultime.

(a) Certificazione ISO 9001

(b) Certificazione ISO 27001

Figura 2.4: Certificazioni ISO di Wintech

2.3 Organizzazione interna

Wintech suddivide le risorse in modo che vi sia una struttura che permetta a figure tecniche e specializzate di lavorare su ambiti ben definiti ed attività elementari. L'organizzazione è divisa in varie divisioni tra cui ***Marketing***, **Commerciale**, **Sviluppo** e **Sistemi**, con ovviamente i reparti di **Risorse Umane** e **Direzione**. Si possono

trovare inoltre gruppi di **Ricerca e Sviluppo** e quelli di **Help Desk**. Ogni unità operativa è gestita da un proprio responsabile, un ***Project Manager***.

2.4 Tecnologie aziendali

Tutta l'azienda si basa su tecnologie di grado *enterprise*, sfruttando principalmente l'ecosistema offerto da Microsoft, ma anche con altri strumenti *open-source*, talvolta gratuiti.

La maggior parte dei dispositivi aziendali utilizza come sistema operativo *Windows 11*, altri *Windows 10* e molti server usano varie versioni di *Windows Server*. Tuttavia sono presenti alcuni dispositivi Apple che montano *MacOS* e alcuni server che operano su sistemi *Linux* delle famiglie *Debian* e *RedHat*, ad esempio *CentOS*.

Per la gestione documentale si affida a *Microsoft Office 365*, mentre per le comunicazioni vengono utilizzati *Microsoft Outlook* per la gestione delle *mail* e *Microsoft Teams* per la messaggistica istantanea e chiamate video e non.

Gli strumenti utilizzati all'interno dell'infrastruttura di rete e per la sicurezza aziendale verranno trattati nel Capitolo 4, in quanto parte integrante della formazione iniziale del percorso di stage.

2.5 Propensione all'innovazione

Come presentato prima nelle sottosezioni 2.1.1 e 2.1.2, Wintech è la prima a proporre soluzioni innovative e all'avanguardia ai propri clienti. La sua capacità di mantenersi aggiornata sulle nuove tecnologie e sfruttando l'esperienza acquisita negli anni, le ha permesso di mantenersi competitiva e rilevante sul mercato.

Tra i vari prodotti offerti e promossi dall'azienda troviamo strumenti per *eLearning*[4] e prodotti di *Enterprise Resource Planning* (ERP)[5]. Due dei punti cardine dei progetti di Wintech sono la *Digital Transformation*[6] e la *Social Collaboration*[7], per sfruttare al meglio le tecnologie digitali ed essere più competitivi sul mercato. Inoltre si cerca di promuovere la comunicazione, la condivisione e la collaborazione tra colleghi, favorendo e aumentando l'*engagement* dei dipendenti e la crescita delle loro competenze, creando un clima confortevole e accogliente all'interno del posto di lavoro.

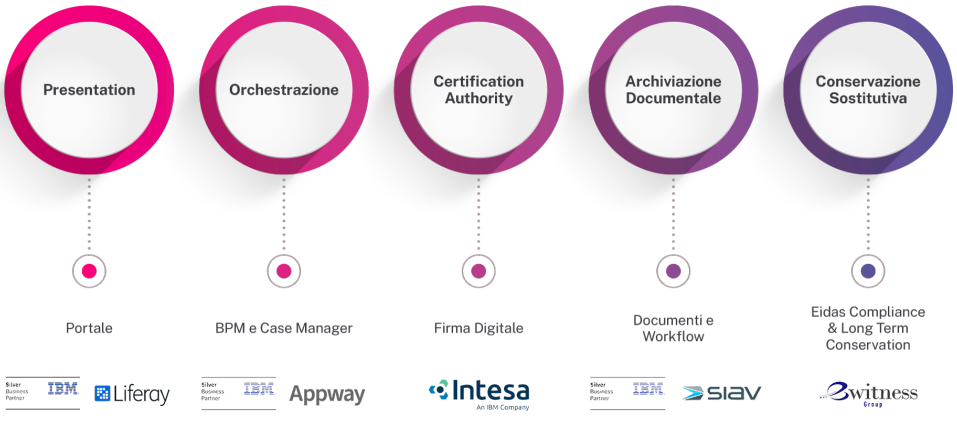


Figura 2.5: Il progetto di *Digital Transformation* di Wintech

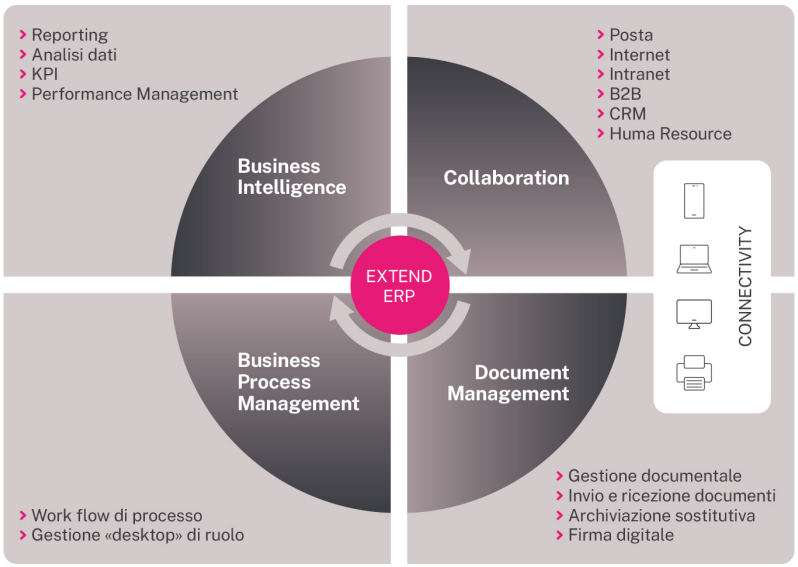


Figura 2.6: Schema di funzionamento di una soluzione *ERP*

2.6 Lo stage nella strategia aziendale

Il mio primo contatto con l'azienda è avvenuto tramite l'evento Stage-IT. Quest'ultimo è stato promosso da Confindustria Veneto Est con i Dipartimenti di Matematica e Scienze Statistiche dell'Università di Padova e partecipato dal Dipartimento di Ingegneria Informatica per favorire l'incontro tra aziende con progetti innovativi nell'ambito IT e studenti dei corsi di laurea in Informatica, Statistica e Ingegneria Informatica interessati allo svolgimento di tirocini. Wintech partecipa all'evento da diversi anni e ha sempre avuto un buon riscontro, sia da parte degli studenti che da parte delle aziende.

Per lo studente lo stage gioca un ruolo importante nella sua formazione e proprio per questo viene consigliato come ultima fase nel percorso universitario, in quanto permette di applicare le conoscenze, sia teoriche che pratiche, ottenute durante il percorso di studi. Inoltre, l'esperienza avuta con il progetto del corso di Ingegneria del Software mette molti alla prova con la necessità di lavorare in un *team* di più persone da coordinare per consegnare un prodotto ad un committente esterno con la necessità di risolvere un problema reale. Inserire dunque uno studente in un contesto aziendale offre al tirocinante la possibilità di "toccare con mano" quello che è il mondo del lavoro, apprendendo dinamiche e processi interni e permettendo di capire se il percorso intrapreso è quello giusto per lui.

Per un'azienda, invece, lo stage è un'opportunità per valutare le capacità degli studenti nel realizzare prodotti con uno scopo pratico e ben definito, non usa e getta. Spesso l'esperienza di stage viene utilizzata anche come strumento per conoscere nuove persone da inserire in organico e non solo ospitando uno studente per due mesi da utilizzare come manodopera a basso costo, ma bensì come un'opportunità per confrontarsi con qualcuno con conoscenze aggiornate e che può portare nuove idee e punti di vista, con un ottica di miglioramento continuo e a lungo termine.

Wintech sotto questo punto di vista propone progetti legati a prodotti che verranno o sono già utilizzati internamente o dai propri clienti. Proprio per questo cerca di instaurare un rapporto con lo stagista fin da subito basato su rispetto e fiducia e

verrà considerato da tutti i dipendenti come un collega a tutti gli effetti. Questo, oltre a fornire un ambiente stimolante e confortevole, responsabilizza il tirocinante a lavorare al meglio per non creare problemi agli altri *team* durante lo sviluppo del proprio progetto.

Per una buona riuscita dello stage è necessario anche un buon rapporto e dialogo tra tutor e stagista. In Wintech si è seguiti e formati con attenzione all'inizio del percorso, in modo da rendersi poi autonomi e riferire in caso di necessità. Questo non significa essere lasciati a se stessi dopo poco, anzi tutti i componenti del *team* in cui si viene inseriti (e non solo) sono disponibili a rispondere a qualsiasi domanda, anche su argomenti non strettamente legati al progetto, e a confrontarsi in caso di problemi o possibili migliorie e soluzioni alternative.

2.7 Scelta dell'azienda

All'evento StageIT tutte le aziende partecipanti esponevano brevemente i progetti che proponevano. Questo mi ha permesso preventivamente di scegliere quelle che più mi interessavano, senza limitare la mia ricerca. Durante tutto il pomeriggio passato nel padiglione della fiera ho cercato di parlare con più aziende possibili, in modo da capire meglio cosa offrissero e quali fossero le loro aspettative, ma anche scoprire progetti non pubblicizzati, essendo le proposte limitate ad un numero massimo di tre.

La maggior parte dei partecipanti erano propositivi e interessati ad avere un colloquio con gli studenti, per capire al meglio le loro capacità e le loro aspettative. Come esperienza mi ha permesso di avere molte piccoli brevi colloqui con responsabili aziendali, grazie ai quali sono riuscito a capire meglio cosa cercare in un'azienda e cosa offrire.

Dopo l'evento ho ricevuto diverse proposte sia da parte di aziende che avevo visitato sia dalle altre, ma dopo l'incontro in sede Wintech per discutere del progetto, ho scelto quest'ultima per la possibilità di lavorare su un campo che mi interessava e diverso da tutte le altre offerte legate principalmente allo sviluppo *software*. Questo mi ha permesso di avere un contatto diretto con il mondo del lavoro, in particolare in un settore che avevo visto solo superficialmente in precedenza durante i periodi di alternanza scuola-lavoro in aziende che offrivano servizi e consulenza in ambito *networking*.

Capitolo 3

Progetto di stage

3.1 Il progetto

Wintech all'evento di StageIT portava tre proposte riguardanti dei progetti legati alle unità di *business* e sviluppo. Durante la breve discussione avuta in fiera, tra i vari dipendenti era presente anche Mirco, del *team* di *network*, con cui è emersa la possibilità di avviare un progetto legato a questo ambito. Dopo un primo scambio di *mail* per capire meglio le esigenze e le possibilità, è stato fissato un incontro in azienda per discutere meglio del progetto con il responsabile e mio futuro tutor Roberto Pezzile.

Nell'ultimo periodo l'azienda si stava informando e analizzando il mercato alla ricerca di uno strumento di NDR da integrare nella propria rete in modo da aumentare le capacità di rilevazione e risposta agli attacchi informatici. Avendo una grande quantità di clienti in *full-outsourcing* che affidano la gestione della propria infrastruttura a Wintech è necessario avere strumenti di sicurezza sempre aggiornati che sfruttano le ultime tecnologie.

Un sistema di NDR è uno strumento che consente di individuare rapidamente i pericoli nella rete e di attuare una *remediation* automatica. Questo monitora costantemente il traffico tramite sonde posizionate in punti strategici e analizza i dati raccolti per identificare eventuali attività sospette o pericolose. In caso di pericolo, il sistema può attivare una risposta automatica o notificare un amministratore, consentendo di rispondere in modo rapido ed efficace ai potenziali attacchi. Questa tipologia di prodotti offre la possibilità di integrarsi con il resto dell'infrastruttura esistente, principalmente con *firewall* e altri componenti di rete, ma anche con *software* presenti sui vari *host*, sia che questi siano *client* o *server*. Lo scopo del progetto è quello di andare a mettere in produzione uno strumento di questo tipo, già individuato dall'azienda, inizialmente come *Proof of Concept* e successivamente come strumento di sicurezza per i clienti in *full-outsourcing*.

Questo particolare tipo di tecnologia viene proposto da aziende affermate sul mercato della strumentazione di rete, ma la scelta di Wintech è stata quella di puntare su *Sangfor*, un nuovo *player* che cerca di affermarsi con prodotti innovativi e competitivi. Tra i principali punti di forza di questa collaborazione si trovano una maggiore economicità ma specialmente la possibilità di instaurare un dialogo molto più diretto con il fornitore rispetto a grandi corporazioni multinazionali dalla lunga storia. Il periodo scelto per lo stage ha permesso inoltre di sfruttare come banco di prova per il sistema l'infrastruttura di un cliente che gestisce strutture ricettive in un periodo di alta stagione, in cui la rete viene messa a dura prova da un gran numero di utenti con esigenze diverse.

Personalmente, ho avuto modo di avere un contatto diretto con esponenti di Sangfor del *team* italiano della sede di Milano, principalmente remoto e digitale e con un'incontro in sede, e con il *team* di supporto remoto asiatico, che si è reso sempre disponibile per risolvere i problemi riscontrati, anche scontrandosi con fusi orari e lingue diverse.

3.2 Vincoli

3.2.1 Vincoli tecnologici

Gli unici vincoli tecnologici posti da Wintech sono stati quelli di utilizzare strumentazione già scelta da loro, dato che il fornitore del prodotto era già stato definito e i vari strumenti di rete erano già in uso, collaudati e non era possibile andare a sostituirli senza una forte motivazione, vista la complessità dell'operazione, sia dal punto di vista tecnico che economico.

3.2.2 Vincoli temporali

Il progetto di stage è stato pianificato per una durata di 320 ore, suddivise in 8 settimane, con un impegno di 40 ore settimanali. Questo ha permesso di avere un quadro generale del lavoro da svolgere e delle tempistiche da rispettare per arrivare ad avere un prodotto configurato e documentato entro le scadenze.

Nella Tabella 3.1 troviamo un prospetto orario suddiviso per le varie fasi del progetto individuate e relativo diagramma di Gantt in Figura 3.1. Queste verranno descritte nel dettaglio nella sezione 3.3.

Fase	**Inizio**	**Fine**	**Ore**
Introduzione ed analisi dello strumento e dell'infrastruttura aziendale	05/06/2023	09/06/2023	40
Deploy e configurazione dello strumento, formazione riguardante tutti gli strumenti necessari per la comprensione delle minacce	12/06/2023	23/06/2023	80
Test del prodotto, analizzando rischi ed attacchi reali e/o simulati	26/06/2023	07/07/2023	80
Configurazione e test delle *remediation*	10/07/2023	21/07/2023	80
Stesura della documentazione interna sulle *feature*, l'installazione e l'utilizzo del prodotto	24/07/2023	28/07/2023	40

Tabella 3.1: Fasi del progetto di stage

3.2.3 Obiettivi e prodotti attesi

Il progetto di stage è stato descritto in obiettivi e prodotti attesi, suddivisi nelle tre categorie obbligatori, desiderabili e facoltativi. Questi sono stati definiti dal tutor aziendale, discussi con lo studente e accettati da entrambe le parti. Tutto il piano, compreso di pianificazione e obiettivi è stato approvato dal tutor accademico.

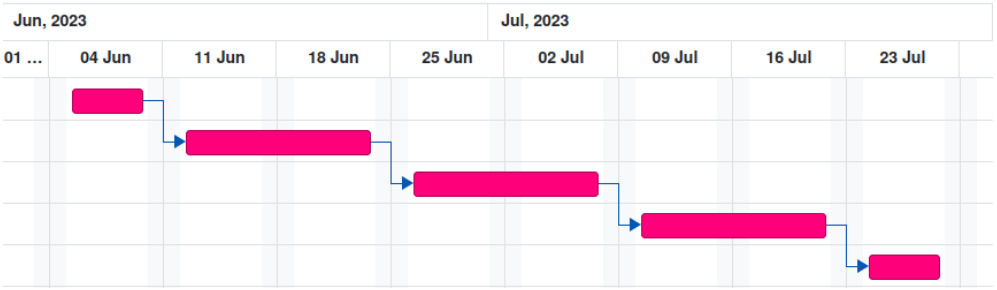


Figura 3.1: Diagramma di Gantt delle fasi del progetto di stage

Obbligatori

In questa categoria troviamo requisiti vincolanti in quanto obiettivi primari richiesti dall'azienda. Ne sono stati individuati cinque e definiti come:

- **O1**: Introduzione ed analisi dello strumento e della infrastruttura aziendale
  - Analisi approfondita delle finalità di uno strumento di NDR
  - Comprensione delle *feature* dello strumento tramite la documentazione del *vendor*
  - Comprensione dell'infrastruttura dove verrà inserita la nuova soluzione
- **O2**: Deploy e configurazione dello strumento, formazione riguardante tutti gli strumenti necessari per la comprensione delle minacce
  - Deploy dello strumento seguendo la manualistica a disposizione
  - Configurazione di base dello strumento e inizio raccolta dei dati
  - Formazione di base sul funzionamento dei principali apparati di *networking* e sicurezza
- **O3**: Test del prodotto, analizzando rischi ed attacchi reali e/o simulati
  - Analisi degli incidenti e degli eventi, calandoli con l'aiuto del tutor e dei colleghi nell'ambiente dov'è stato installato
  - Predisporre ed attuare simulazioni di varie tipologie, analizzando la risposta dell'NDR
- **O4**: Configurazione e test delle *remediation*
  - Analisi delle *feature* di *remediation* tramite documentazione del fornitore
  - Integrazione dell'NDR con il *software* di EDR al fine di attuare azioni di *remediation*
  - Configurazione delle *policy* di *remediation* e svolgimento di test su alcuni *client*
- **O5**: Stesura della documentazione interna sulle *feature*, l'installazione e l'utilizzo del prodotto

I prodotti attesi per questi obiettivi sono:

- Documentazione sullo strumento e sulle sue *feature*
- Documentazione sull'infrastruttura aziendale
- Documentazione sul *deploy*, sulla configurazione e sull'utilizzo dello strumento
- Documentazione sulle simulazioni di pericolo svolte sull'NDR e documentazione degli esiti riscontrati

Desiderabili

Questa categoria raccoglie requisiti non strettamente necessari ma che portano un riconoscibile valore aggiunto al termine del progetto. Ne sono stati individuati tre e definiti come:

- **D1**: Raggiungere l'autonomia nella ricerca delle informazioni di sicurezza e di *networking* tramite gli strumenti aziendali
  - Revisione della configurazione per operare migliorie
  - Documentare il *setup* e le migliorie attuate
- **D2**: Documentare le simulazioni di pericolo svolte sull'NDR e documentare gli esiti riscontrati
- **D3**: Integrare ulteriori apparati nell'infrastruttura NDR, al fine di espandere le capacità di *remediation* (*Firewall*, *WAF*, etc.)

I prodotti attesi per questi obiettivi sono:

- Individuato quali attacchi vengono rilevati e come il prodotto li segnala

Facoltativi

In questa categoria sono presenti dei requisiti opzionali che rappresentano un valore aggiunto non strettamente competitivo. Ne sono stati individuati due e definiti come:

- **F1**: Attuare manualmente delle operazioni di *remediation* ad alcune anomalie individuate
  - Individuare come *bypassare* i controlli dell'NDR, simulando un attacco che non viene rilevato
- **F2**: Attivazione globale delle *remediation* automatiche a tutti i *client* e all'intero ambiente

I prodotti attesi per questi obiettivi sono:

- Individuato come *bypassare* la sicurezza offerta dal prodotto

3.3 Pianificazione

Lo stage è iniziato il 5 giugno 2023 e si è concluso il 2 agosto 2023, sforando di due giorni lavorativi quanto pianificato. La causa del ritardo è dovuta ad alcune mie assenze per motivi personali e partecipazioni ad alcuni esami universitari, entrambe situazioni che non sono state da me considerate nella pianificazione iniziale. In retrospettiva, sarebbe stato opportuno valutare un periodo di *buffer* per eventuali imprevisti, ma nonostante questo il progetto è stato portato a termine, impiegando le trecentoventi ore previste.

Il carico di lavoro quotidiano è stato di otto ore, un impegno *full-time*, svolte nell'ufficio della sede di Padova dalle ore 9:00 alle ore 18:00, con un'ora di pausa pranzo.

Il percorso di stage è stato suddiviso in cinque macro fasi principali, in modo da avere un quadro generale del lavoro da svolgere e delle tempistiche da rispettare. Queste fasi sono state individuate come:

3.3.1 Fase 1: Introduzione ed analisi

Definita come *«Introduzione ed analisi dello strumento e dell'infrastruttura aziendale»* e pianificata per durare la prima settimana.

Per permettere allo studente di comprendere il contesto aziendale, è stato previsto un periodo di formazione iniziale, in cui sono stati presentati i vari reparti aziendali e le tecnologie utilizzate. In particolare è stata fatta una panoramica delle *feature* e capacità dei vari prodotti NDR presenti sul mercato, per capire in cosa quello proposto da *Sangfor* si differenziasse dagli altri. Inoltre, è stata descritta l'infrastruttura aziendale, in particolare la rete interna e quella dei servizi offerti ai clienti in *full-outsourcing*, in modo da comprendere come i vari prodotti si integrassero tra loro, sia quelli di sicurezza che i vari servizi *cloud*.

3.3.2 Fase 2: Deploy e configurazione

Definita come *«Deploy e configurazione dello strumento, formazione riguardante tutti gli strumenti necessari per la comprensione delle minacce»* con una durata prevista di due settimane.

In questa fase le sonde *STA* sono state inserite nella rete aziendale e configurate per la rilevazione del traffico e degli attacchi informatici. Con lo strumento configurato e attivo si è andati ad operare con esso per capire come questo ragiona, documentando le varie *feature* e le capacità di rilevazione e individuate e proponendo migliorie dove possibile.

Per la natura del prodotto che punta ad integrarsi con l'infrastruttura esistente, in questa fase è stata anche effettuata della formazione sugli strumenti di rete e sicurezza informatica utilizzati in azienda, quali *firewall*, *switch*, sistemi di monitoraggio e *antivirus*, in modo da comprendere come correlare le informazioni raccolte dalle sonde *STA* con quelle di altri strumenti.

3.3.3 Fase 3: Test del prodotto

Definita come *«Test del prodotto, analizzando rischi ed attacchi reali e/o simulati»* con una durata prevista di due settimane.

In questa fase è stato testato il prodotto, simulando attacchi e verificandone la capacità di rilevazione e di risposta. Inoltre, si è analizzato come il sistema correla

le informazioni raccolte dalle sonde *STA* con quelle ottenute da altri strumenti di sicurezza informatica.

Tutte le informazioni raccolte sono state documentate in modo da formare la base per la fase successiva. Le *detection policy* definite in questa fase si limitavano a rilevare gli attacchi, classificarli e andare a definire delle *whitelist* per evitare falsi positivi, senza però agire automaticamente ma solamente notificando gli amministratori di rete.

3.3.4 Fase 4: Configurazione e test delle remediation

Definita come *«Configurazione e test delle remediation»* con una durata prevista di due settimane.

In questa fase sono state configurate le *remediation* per gli attacchi rilevati, definendo delle *automatic response* per le situazioni malevole raccolte nella fase precedente in modo da far agire il sistema autonomamente per i casi più semplici. Questa fase più di tutte le altre necessita di configurare l'interazione della piattaforma NDR con gli altri strumenti, in modo da poter agire in modo efficace e coordinato.

3.3.5 Fase 5: Documentazione

Definita come *«Stesura documentazione»* con una durata prevista di una settimana.

Al termine del percorso di stage è stato documentato tutto il lavoro svolto, in modo da poter essere utilizzato come base per il futuro. In particolare, sono state raccolte le *detection policy* e le *automatic response* definite, insieme a delle *best practice* scoperte per l'utilizzo del prodotto, in modo da poter essere utilizzate per la formazione di nuovi dipendenti.

Capitolo 4

Tecnologie utilizzate

Di seguito una descrizione dettagliata di come mi sono approcciato allo stage, dalla formazione all'implementazione degli obiettivi richiesti.

4.1 Studio degli ambiti di interesse e del dominio tecnologico

Durante la prima settimana dello stage, affiancato da Mirco, ho ripassato e approfondito tutti i concetti legati al mondo delle reti, dalle basi del protocollo TCP/IP, del funzionamento e delle topologie di rete a livello fisico, fino ad arrivare ai protocolli di livello applicativo, di uso comune come HTTP, FTP e SSH (e tutte le loro controparti sicure con SSL) e nuove proposte come QUIC.

Sono stati discussi i concetti di indirizzamento IP, di *subnetting* e di routing, sono stati approfonditi i concetti di NAT e di *firewall*, e tutto ciò che concerne la sicurezza informatica e la protezione dei dati.

Dal lato pratico sono stati utilizzati strumenti come *Wireshark*, per l'analisi del traffico di rete, e *Nmap*, per la scansione delle porte di un *host*. Per prendere confidenza con le configurazioni degli apparati di rete utilizzati dall'azienda mi sono stati messi a disposizione alcuni strumenti tra cui un *Mikrotik RouterBoard*, un *Watchguard Firebox* e uno *switch HP ProCurve*, dove avevo accesso completo e libertà di gestione.

Con questi ho potuto sperimentare le configurazioni di base di un *firewall*, di un *router* e di uno *switch*, e ho potuto sperimentare la configurazione di VLAN e di VPN, utilizzando vari portatili per simulare degli *host* e le loro interazioni in rete.

I vari attacchi e le mitigazioni discusse in questo periodo verranno approfondite nella Appendice B per non appesantire il flusso della relazione.

4.1.1 Protocolli analizzati

IP

Il protocollo IP è stato il primo protocollo analizzato. Sono stati ripassati i concetti di indirizzamento IP, di *subnetting* e di *routing*. Per poter lavorare efficacemente sui *log* e per riconoscere velocemente le sorgenti e le destinazioni delle trasmissioni che il sistema rilevava è stato necessario ripassare le classi IP e le categorie riservate

Subnetting

Lavorando su una rete complessa come quella di un'azienda è necessario suddividere la rete in sotto reti, per poter gestire in modo più semplice le risorse e per poter applicare delle regole di sicurezza più specifiche, limitare il traffico *broadcast* nella rete e gestire in modo puntuale la visibilità delle risorse. Sfruttando la rete interna come esempio mi è stato spiegato come andare a definire regole di accesso e permessi per i vari reparti.

NAT

Il NAT (*Network Address Translation*) è il protocollo che permette di modificare gli indirizzi, sia sorgente che destinazione, di una connessione durante il transito su un apparato. Solitamente questo avviene nel *firewall*, che sfrutta le *porte* per ricordare queste modifiche. Proprio per questo utilizzo "improprio" dello strumento delle porte, questa metodologia viene considerata come il "livello 3.5" dello *stack ISO/OSI*. Questo protocollo ha tre tipologie di configurazione:

- *Dynamic NAT (DNAT)*: permette di mappare un indirizzo IP privato ad un indirizzo IP pubblico, in modo che tutti i pacchetti che arrivano all'indirizzo pubblico vengano instradati all'indirizzo privato. Questo tipo di configurazione è utile quando si hanno più *host* che devono accedere ad Internet, ma non è necessario che siano raggiungibili dall'esterno.
- *Static NAT (SNAT)*: viene utilizzato per dare accesso ad esterni alla rete interna. Detto anche *port-forwarding* perché agisce con un meccanismo che alla ricezione di un pacchetto dall'esterno instrada quest'ultimo verso una coppia *IP:PORT* dietro al *firewall*.
- *NAT Loopback (UNAT)*: permette al *router* di instradare internamente le richieste da un dispositivo sulla rete locale che contatta un altro tramite l'IP esterno, senza dover uscire dalla rete e rientrare.

Domain Controller e Active Directory

In Wintech tutti utilizzano sistemi *Windows*. Questo permette di avere un'infrastruttura di rete molto semplice da gestire, grazie all'utilizzo di *Active Directory* e di *Domain Controller*. Questi strumenti permettono di gestire in modo centralizzato tutti gli utenti e i loro permessi, e di applicare delle regole di sicurezza a livello di rete, come ad esempio la richiesta di autenticazione per accedere a una risorsa condivisa o ad un apparato di rete, come *firewall* o *switch*.

Il mio account, ad esempio, era stato configurato in modo da avere tutti i permessi di amministratore locale sulla mia macchina, ma con l'accesso ai soli file e cartelle comuni a tutti i dipendenti e quelle legate al *team* di rete.

RADIUS e 802.1X Authentication

Il portatile che mi è stato fornito disponeva sia di una scheda di rete *wireless* che di una porta *Ethernet*. La rete aziendale è suddivisa in varie VLAN, tutte protette da autenticazione. Sfruttando il fatto che tutti i dispositivi sono già autenticati tramite *Active Directory* e grazie all'utilizzo di un server che supporta il protocollo *RADIUS*, è possibile autenticare utenti e dispositivi sfruttando un certificato che il dominio fornisce, permettendogli di accedere alle reti di cui hanno il diritto di utilizzo dopo una validazione di quest'ultimo.

HTTP e HTTPS

Vista la presenza di molti applicativi interni e di clienti con interfacce *web* è stato utile ripassare la struttura del protocollo HTTP. A volte, essendo questi servizi offerti solo ai dipendenti che operano in un'infrastruttura di rete interna e controllata a monte, non viene utilizzata la versione sicura, rendendo quindi il contenuto delle richieste e delle risposte in chiaro.

Lo strumento di NDR che sono andato ad utilizzare aveva le proprie sonde inserite all'interno di questa rete e mi ha permesso di capire quanto, in una situazione del genere, per un attaccante con accesso locale sia facile intercettare e manipolare il traffico di rete.

Uno degli attacchi analizzati legati al protocollo HTTP è descritto nella sezione B.1.

FTP, SFTP e FTPS

Per quanto riguarda i protocolli di trasferimento di *file*, ho potuto approfondire le differenze tra FTP, SFTP e FTPS. L'ultimo protocollo è stato rilevato casualmente dal sistema, essendo poco utilizzato rispetto alla sua altra versione sicura SFTP.

- *FTP*
  - Non supporta la cifratura
  - Autenticazione con *username* e *password* in chiaro
  - Non supporta i certificati
  - Nei *firewall* è necessario aprire più porte per gestire la versione attiva e passiva, dove vengono utilizzati più canali per la connessione e il passaggio dei dati
- *FTPS*
  - Sfrutta TLS/SSL per rendere sicuro il trasferimento. Tuttavia è possibile che sià definita una strategia di *fallback* alla sua versione non sicura, rendendo il trasferimento in chiaro
  - Utilizzando SSL/TLS è possibile utilizzare certificati X.509 per l'autenticazione del *server* e del *client*
  - Per sua natura, essendo un protocollo che utilizza più canali per la connessione e il passaggio dei dati, è necessario aprire più porte nei *firewall*.
  - Operando su più canali c'è una piccola probabilità che FTPS sia più veloce di SFTP. Tuttavia la differenza è minima e spesso trascurabile.
- *SFTP*
  - Il trasferimento avviene all'interno di un tunnel SSH. Se questo non viene instaurato non c'è possibilità di *fallback* alla versione non sicura.
  - L'autenticazione avviene tramite chiavi SSH, spostando il problema della sicurezza sulle chiavi stesse.
  - Lavorando all'interno di un tunnel SSH è necessario aprire una sola porta nei *firewall*, rendendo più semplice la configurazione.

DNS

Il protocollo DNS è stato ripassato per poter capire come funzionano i domini e come vengono risolti gli indirizzi IP. Questo mi ha permesso di analizzare poi degli attacchi come quello di *DNS Amplification* (sezione B.2) e tecniche di mitigazione offerte dai *firewall* come la *DNS Sinkhole* (sezione B.3). Tramite il *Domain Name System*, vengono convertiti *hostname* del tipo `example.com` nell'indirizzo IP corrispondente, dove andare poi a collegarsi.

SNMP e LLDP

SNMP (*Simple Network Management Protocol*) e LLDP (*Link Layer Discovery Protocol*) sono due protocolli che permettono di gestire e monitorare i dispositivi di rete. Il primo permette di raccogliere informazioni sullo stato dei dispositivi, mentre il secondo permette di scoprire i servizi disponibili in una rete senza ricorrere a DHCP o DNS.

Il primo è stato utilizzato insieme al software di monitoraggio *PRTG Monitor* per raccogliere informazioni sullo stato dei dispositivi di rete. Il secondo, essendo attivo di default su *Windows 11* è stato utilizzato nella rete interna dato che i dispositivi che utilizzano questo sistema operativo in azienda sono la maggioranza.

Entrambi i protocolli non sono sicuri per natura, anche se in realtà SNMPv3 supporta strumenti di sicurezza. Sono stati utilizzate le versioni insicure per mantenere la maggiore compatibilità possibile.

Il sistema NDR quindi segnalava molti dispositivi che utilizzavano questi protocolli, in quanto potenzialmente vulnerabili, nonostante il comportamento fosse quello effettivamente atteso, e sono state quindi create delle *whitelist* per evitare falsi positivi.

Redfish

Redfish è uno standard che raccoglie una serie di specifiche che permettono di gestire in modo i dispositivi di rete sfruttando interfacce *RESTful*. Durante lo stage si è provato ad integrare in alcuni sensori di monitoraggio ma non è stato possibile per mancanza di compatibilità con i dispositivi utilizzati.

QUIC

Riscontrato tramite l'utilizzo di *Wireshark*, mi sono documentato sul protocollo QUIC[8], che è stato sviluppato da *Google* per migliorare le prestazioni di HTTP/2, con lo scopo di essere quasi equivalente ad una connessione TCP ma con latenza ridotta. Utilizza UDP per le sue comunicazioni, e permette di gestire in modo più efficiente la perdita di pacchetti e la congestione della rete. Permette inoltre di gestire in modo più efficiente la sicurezza, utilizzando TLS per la cifratura e l'autenticazione, ma spostandone lo scambio di chiavi all'interno dell'*handshake* iniziale, rendendo più veloce la connessione.

4.1.2 Programmi utilizzati

VLAN

Utilizzando lo *switch HP ProCurve* fornitomi ho potuto sperimentare la configurazione di VLAN. Tramite questa tecnica è possibile suddividere una rete fisica in più reti logiche, che possono essere gestite in modo indipendente. Questo permette di ridurre in primo luogo il numero di apparati fisici necessari, e in secondo luogo di applicare

delle regole di sicurezza più specifiche, in modo da limitare l'accesso sulla base della rete a cui si è connessi.

Tutto questo avviene a livello due dello stack ISO/OSI, tramite l'assegnazione di un *tag* VLAN ad ogni pacchetto, secondo lo standard 802.1Q, che viene utilizzato dagli *switch* per instradare il traffico verso la rete corretta. Il *tag* del pacchetto segue la configurazione data ad ogni porta dello *switch*: queste vengono dette *tagged* (o *trunk*) se sono in grado di gestire più VLAN, oppure *untagged* (o *access*) se accettano solo pacchetti della VLAN corretta, venendo quindi utilizzate per collegare gli *host* finali, a differenze delle prime che permettono di collegare gli *switch* o altri apparati come *server*, *access point* e *firewall* tra loro.

Wireshark

Wireshark è uno dei principali programmi utilizzati per l'analisi del traffico di rete. Permette di catturare tutti i pacchetti che transitano su una rete e visualizzarne i contenuti. Si possono filtrare i pacchetti in base a diversi criteri, come ad esempio il protocollo utilizzato, l'indirizzo IP sorgente o destinazione, la porta sorgente o destinazione, e tanti altri filtri. Inoltre è possibile analizzare il traffico in tempo reale, e di visualizzare statistiche sulle comunicazioni, come ad esempio il numero di pacchetti per protocollo o per indirizzo IP, il numero di *byte* per protocollo e molti altri.

Durante il periodo di stage sono stati segnalati alcuni problemi legati alla ricezione delle chiamate dai telefoni *VoIP* aziendali e utilizzando la funzionalità di seguire flussi di connessioni in *Wireshark* ci ha permesso di capire chiaramente in quale fase del *setup* della chiamata si presentava il problema. Questo mostra la versatilità dello strumento, non limitata alle solo connessioni *web* ma ogni tipo di comunicazione che avviene su una rete. È possibile inoltre sfruttare questo programma per analizzare traffico che passa attraverso interfacce USB.

Figura 4.1: Logo di Wireshark

Nmap

Nmap, *Network Mapper*, è uno strumento *open-source* utilizzato per effettuare scansioni e analizzare le reti. È uno strumento potente che consente di esaminare le reti e individuare dispositivi, porte aperte, servizi in esecuzione e altre informazioni rilevanti.

Durante il mio stage mi è stato presentato come uno degli strumenti di base che possono tornare utili in varie occasioni, vista la sua versatilità. Ho avuto modo di utilizzarlo per verificare le configurazioni che definivo sul *RouterBoard Mikrotik* e sul *firewall* di *Watchguard*, sia di test che alcune in produzione per chiarire perché alcuni dispositivi riuscissero a raggiungere altri in reti diverse.

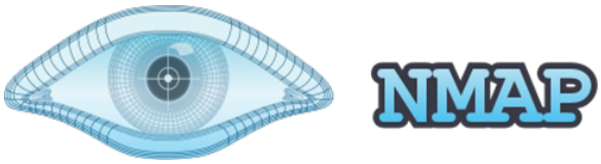


Figura 4.2: Logo di Nmap

PRTG Monitor

Come strumento di monitoraggio dei vari dispositivi e servizi dislocati per tutta la rete aziendale, in Wintech viene utilizzato *PRTG Monitor*, prodotto da PAESSLER. Questo programma permette di catalogare e monitorare ogni elemento dell'infrastruttura, dai server ai servizi, dalle stampanti ai dispositivi di rete, e di visualizzare in tempo reale lo stato di ogni elemento. Permette di impostare delle soglie di allarme, in modo da essere avvisati in caso di problemi, e di visualizzare statistiche sulle prestazioni di ogni elemento. Permette inoltre di creare delle mappe di rete, che mostrano la topologia della rete e lo stato di ogni elemento, e di creare dei *report* che mostrano le statistiche di un periodo di tempo.

Per la gestione dell'NDR sono stati aggiunti i dispositivi dove sono state installate le sonde e configurati i sensori per monitorare lo stato dei NUC fisici e del servizio di rilevazione del traffico. In alcuni casi i sensori interni al programma non erano sufficienti e quindi ho aiutato a costruire dei sensori personalizzati, creando degli *script* in *Python* e *Powershell* che andavano a interrogare i dispositivi e a restituire i dati richiesti, tramite file strutturati in XML per dare modo ai sensori di segnalare i dati correttamente e le violazioni delle soglie impostate.

Ad esempio, uno *script* a cui ho lavorato per questo programma si occupava di monitorare il corretto aggiornamento del tecnico reperibile nel sistema di *ticketing* aziendale. Scritto in linguaggio *PowerShell*, interrogava il sistema e recuperava tramite *API REST* lo stato del tecnico reperibile e andava a verificare che questo fosse aggiornato correttamente, segnalando un errore nel caso in cui non fosse presente o presentasse un errore.

Figura 4.3: Logo di PRTG Monitor

Mikrotik RouterOS

Il *RouterOS* è un sistema operativo basato su *Linux* sviluppato da *Mikrotik* per i suoi apparati di rete. Questo sistema operativo permette di configurare in modo semplice e veloce tutti i dispositivi di rete, tramite un'interfaccia grafica o tramite un terminale. Permette di configurare e adoperare molti protocolli di rete. Inoltre è possibile di configurare un *firewall* per proteggere la rete, un *server* DHCP e di configurare un *hotspot* per fornire accesso alla rete a chiunque si connetta.

Ho utilizzato questo sistema per costruire una piccola rete e collegare vari dispositivi dove effettuare dei test e per sperimentare le configurazioni di base di un *router* e di uno *switch*.

Figura 4.4: Logo di Mikrotik

Watchguard System Manager

Come introduzione per capire il funzionamento dei *firewall* ho utilizzato un *Firebox* di *Watchguard*, fornito da Wintech, e il software *Watchguard System Manager*, che permette di configurarlo e di monitorarne lo stato. Permette di configurare le regole di NAT e *allow/deny*, configurare le VPN, cosa che ho fatto sia nelle mie configurazioni di test che in alcune configurazioni di clienti in produzione.

Figura 4.5: Logo di Watchguard

Per avere una panoramica completa sui vari prodotti presenti e offerti sul mercato, ho potuto vedere anche altri *firewall* utilizzati in azienda, come ad esempio quelli di *Palo Alto*, in modo da capire come questi si differenziano tra loro.

Putty

PuTTY è un *client open-source* per collegamenti SSH, telnet e seriali, sviluppato originariamente per la piattaforma *Windows*, che permette di superare le limitazioni del terminale di Microsoft. Permette di collegarsi a un *host* e di gestire la connessione tramite un'interfaccia grafica. Tramite questo programma mi sono potuto collegare con un cavo RS-232 ai vari dispositivi di rete con un collegamento seriale, agendo direttamente sul sistema operativo e configurando i vari servizi.

Figura 4.6: Logo di Putty

cURL

cURL è un programma *open-source* che permette di effettuare richieste di vari protocolli, configurando ogni aspetto della richiesta, come ad esempio il metodo, l'*header*, i parametri, e molti altri. Permette inoltre di salvare la risposta in un *file*, di seguire i *redirect*, e di impostare un *timeout*. Permette inoltre di effettuare richieste in modo parallelo o in modo ricorsivo, andando a seguire i *link* presenti nella risposta. Un suo grande vantaggio nei test è che non utilizza *cache*, che a volte falsifica i risultati portando a falsi negativi o positivi

Figura 4.7: Logo di cURL

Notepad++

Per la gestione dei *file* di testo, ha sostituito il classico *Blocco Note* di *Windows* con il programma *open-source Notepad++* . Permette di gestire più *file* contemporaneamente, di evidenziare la sintassi di molti linguaggi di programmazione, e di muovermi velocemente all'interno di grossi file di *log*.

Figura 4.8: Logo di Notepad++

Capitolo 5

Analisi del prodotto

Di seguito un'analisi del prodotto Sangfor CyberCommand, con cui ho lavorato durante il mio stage.

5.1 Homepage e dashboard

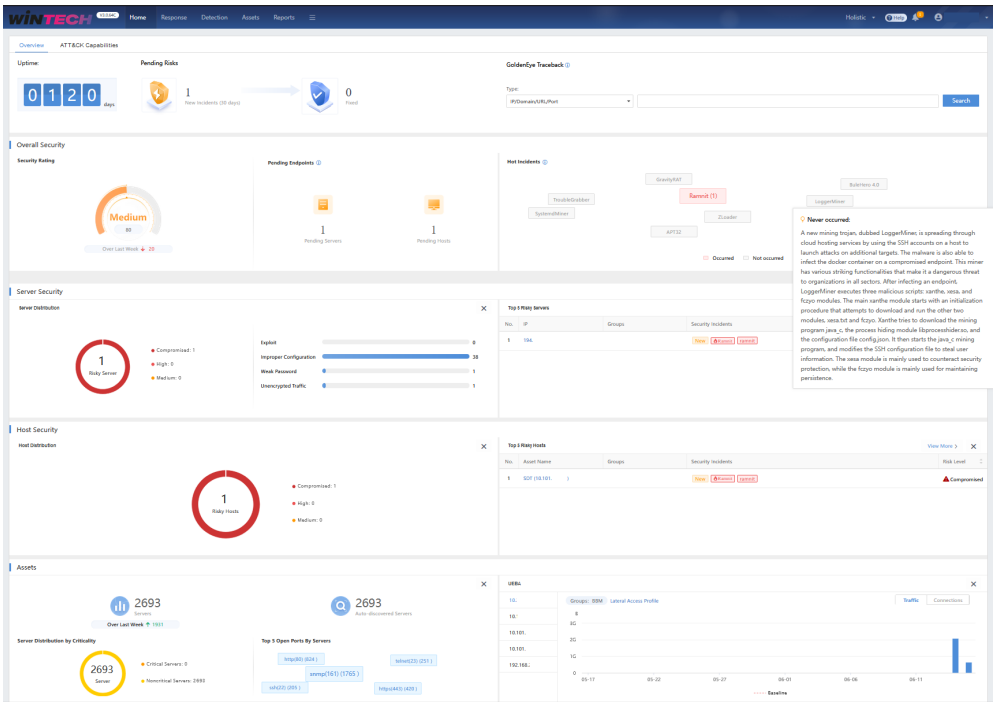


Figura 5.1: Home page del CyberCommand

Analizziamo nel dettaglio i vari elementi presenti nella pagina principale del CyberCommand, mostrata in Figura 5.1.

- *Menu di navigazione*: permette di navigare tra le varie pagine del sistema e di accedere alle varie funzionalità.
- *Uptime*: mostra da quanto il sistema è in esecuzione e un contatore delle segnalazioni riscontrate.

5.1.1 Overall Security

Mostra un indice di sicurezza (Figura 5.2), su una scala da 0 a 100, calcolato in base a quanti dispositivi tra *server* e *host* monitorati sono classificati come vulnerabili o compromessi.

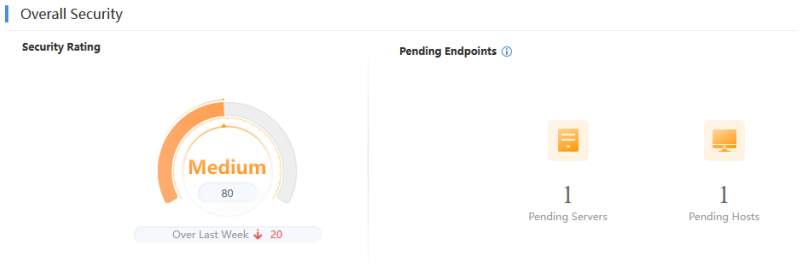


Figura 5.2: Sezione di *Overall Security*

5.1.2 Server Security

Mostra la quantità di errori rilevati in un dato momento, catalogati secondo quattro categorie. In Figura 5.3 vediamo che viene mostrata in maniera molto simile alla sezione di *Overall Security*. Le categorie sono:

- *Exploit e vulnerabilità*
- *Weak Password*: il sistema valuta le *password* che riesce a estrarre dal traffico in chiaro. Se queste non superano un controllo basato su dei requisiti minimi di sicurezza o sono contenute in una lista di *password* deboli viene segnalato un errore
- *Unencrypted Web Traffic*: se è il sistema rileva del traffico in chiaro lo segnala e propone alcune soluzioni per risolvere il problema
- *Improper configuration*: segnala la presenza di configurazioni note per essere rischiose, come ad esempio porte aperte che non dovrebbero esserlo

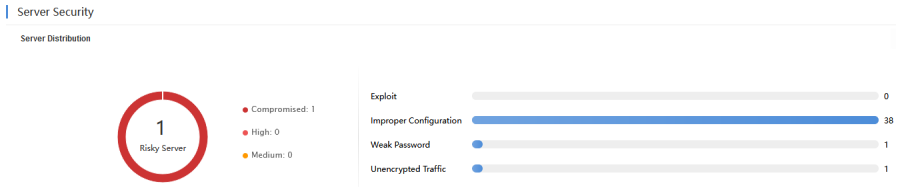


Figura 5.3: Sezione di *Server Security*

5.1.3 Host Security

Durante la scansione dei vari pacchetti, se questi vengono classificati dal sistema come parte di uno scambio malevolo, gli *host* che li hanno inviati o ricevuti vengono segnalati come compromessi. Vengono separati per gravità dell'incidente, come in Figura 5.4.

Figura 5.4: Sezione di *Host Security*

5.2 Segnalazioni

Il sistema categorizza le segnalazioni in tre livelli di gravità.

5.2.1 Incident

Si tratta di eventi correlati a possibili attacchi. Il CyberCommand mostra anche a quale fase dell'attacco è arrivato. Le fasi mostrate in Figura 5.5 seguono quelle definite nella matrice MITRE ATT&CK[9].

Figura 5.5: Fasi dell'attacco in una segnalazione *Incident*

5.2.2 Alert

Si tratta di eventi che non vengono direttamente collegati ad un possibile attacco ma che il sistema considera necessario analizzare perché sospetti.

5.2.3 Weakness

Qui vengono catalogati tutti i problemi rilevati dal sistema. Sono divisi nelle categorie discusse nella sottosezione 5.1.2.

5.2.4 Analisi del traffico

La maggior parte degli strumenti di sicurezza di Sangfor si basano su *Neural-X* [10], un sistema di analisi *cloud-based* che sfrutta le risorse dei *team* composti da *Data Scientist*, *White Hat Researcher* e *Security Analyst*, insieme ad un sistema di intelligenza artificiale. Questo permette di essere sempre aggiornati sulle ultime minacce e di rilevare anche quelle sconosciute, che non sono ancora state catalogate, tramite l'analisi del comportamento del traffico e dei dispositivi.

Avere uno strumento che riesce a riconoscere in automatico e segnalare il più velocemente possibile ogni minaccia è molto importante, in quanto permette di andare a coprire anche i "punti ciechi" nella rete, dove spesso si notano gli attacchi quando questi sono già in uno stadio avanzato.

Tuttavia, queste analisi devono essere poi raffinate e adattate al contesto specifico in cui vengono utilizzate, in quanto non sempre il comportamento di un dispositivo è malevolo. Ad esempio, un dispositivo che si connette ad un *server* per scaricare un aggiornamento potrebbe essere segnalato come un tentativo di *data exfiltration*, ma in realtà è un comportamento normale e non deve essere segnalato come un problema. Altri esempi sono dispositivi che per loro natura utilizzano protocolli in chiaro e insicuri, per un semplicità e compatibilità, per monitoraggio o test di raggiungibilità. Anche i reparti di sviluppo e test possono essere segnalati come sospetti, in quanto spesso utilizzano ambienti di sviluppo che non rispettano tutte le migliori pratiche di sicurezza, essendo ambienti di test, già racchiusi in una rete sicura e non esposti all'esterno.

5.3 Tipologie di problemi rilevati

Tutti i problemi rilevati dal sistema vengono catalogati come *Alert*, che a loro volta possono scatenare un *Risk*. Quando un dispositivo è legato ad uno o più *Risk*, viene segnalato un *Incident* per indicare una possibile compromissione del determinato *host*.

5.3.1 Alert

Questa tipologia di problemi raccoglie eventi che il sistema non considera attacchi ma che potrebbero essere sospetti. Non vengono mostrati nella *dashboard* principale fino a che non scatenano un *Risk*.

In Figura 5.6 possiamo vedere una lista di *Alert*.

5.3.2 Risk

In un *Risk* vengono descritti quali problemi sono stati rilevati (*Threat*), la direzione dell'attacco, il punto nelle fasi del MITRE e lo stato attuale, se risolto o meno. Come mostrato in Figura 5.7, per avere un'idea più precisa è presente un grafico dell'andamento nel tempo e da quale sonda è stata rilevata la minaccia.

In ottica di integrazione con gli altri strumenti di Sangfor, viene anche segnalata la presenza dell'*Endpoint Secure* sul dispositivo interessato.

5.3.3 Incident

Negli *Incident* vengono raccolti tutti gli attacchi legati un determinato problema, segnalando gli *host* che lo hanno subito e la gravità di esso.

No.	Last Detected	Threat	Threat Type	Attack Stage
1	2023-07-27 10:54:50	DCSync request initiated by a...	DRS Command E...	Propagation
2	2023-07-27 10:54:03	Information Disclose Admin ...	Web Component ...	Exploitation
3	2023-07-27 10:53:48	DCSync request initiated by a...	DRS Command E...	Propagation
4	2023-07-27 10:50:04	Weak Web password	Web Weak Passw...	Weaknesses
5	2023-07-27 10:48:50	DCSync request initiated by a...	DRS Command E...	Propagation
6	2023-07-27 10:41:41	Access to malicious domain n...	Trojan	C&C
7	2023-07-27 10:41:41	Access to malicious domain na...	Trojan	C&C
8	2023-07-27 10:31:26	Weak SNMP password	SNMP Weak Pass...	Weaknesses
9	2023-07-27 10:28:50	Access to malicious domain n...	Trojan	C&C
10	2023-07-27 10:28:50	Access to malicious domain n...	Trojan	C&C
11	2023-07-27 10:28:50	Access to malicious domain n...	Trojan	C&C
12	2023-07-27 10:27:44	Access to malicious domain n...	Trojan	C&C
13	2023-07-27 10:22:48	DS_ Store Information Disclo...	OS Kernel Exploit	Exploitation
14	2023-07-27 09:44:25	Fast brute-force encryption a...	Brute-Force Acco...	Propagation
15	2023-07-27 09:36:52	Libsys Oracle Dbconfig Leak ...	Web Framework ...	Propagation
16	2023-07-27 09:32:44	Fast brute-force attack on SSH	Brute-Force Attac...	Reconnaissance

Figura 5.6: Lista di vari *Alert* rilevati

Figura 5.7: Dettaglio di *Risk*

In Figura 5.8 possiamo vedere un *Incident* legato ad una infezione dovuta ad un *ramnit worm*.

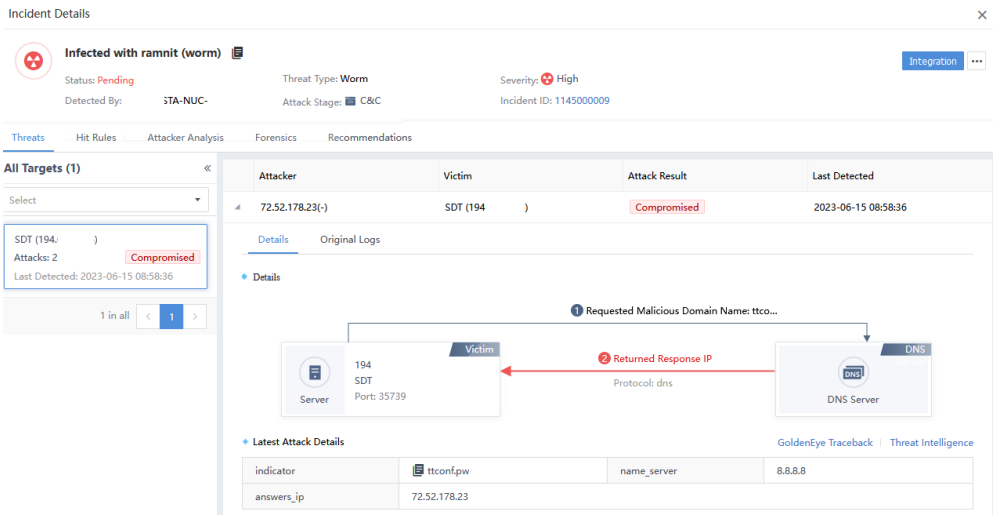


Figura 5.8: Dettaglio di *Incident*

Qui ci viene presentato anche un grafico che ci mostra come l'attacco si è propagato, tra quali dispositivi e in che direzione. In questo caso, essendo legato ad una richiesta DNS, vengono mostrati mostrato anche il dominio e i vari IP coinvolti.

5.3.4 Flusso di analisi

Tutto il traffico che le sonde captano viene analizzato solo dopo essere passato attraverso una serie di filtri contenenti una delle *whitelist*, permettendo all'amministratore di sistema di andare a definire cosa non è necessario analizzare. Questo meccanismo è stato utilizzato per evitare di ricevere segnalazioni legate a strumenti che operano per loro natura con protocolli in chiaro, considerati dall'NDR come insicuri, in modo da limitare il numero di falsi positivi. In Figura 5.9 in che ordine i filtri vengono applicati.

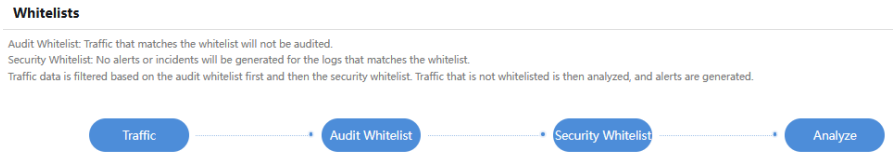


Figura 5.9: Flusso di analisi del traffico

Audit Whitelist

Tramite questa funzionalità tutto il traffico che corrisponde a un certo criterio viene ignorato. Questo è stato utilizzato per evitare di ricevere segnalazioni legate ad esempio a collegamenti noti di cui non era necessario tracciare il traffico, come ad esempio alcune richieste di aggiornamento tra i vari strumenti di monitoraggio verso gli altri dispositivi. Il *form* di definizione di una nuova regola è mostrato in Figura 5.10.

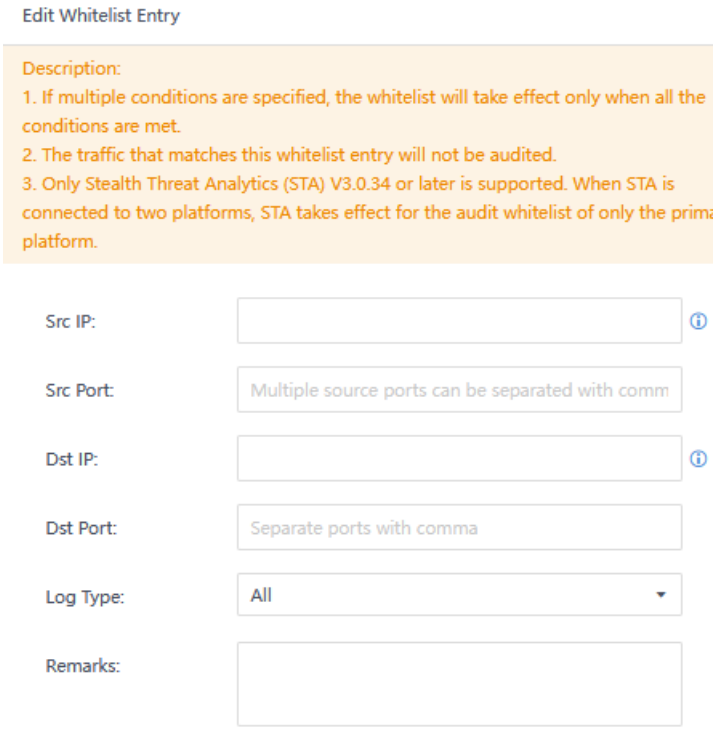


Figura 5.10: Definizione di una *Audit Whitelist*

Security Whitelist

Tutto il traffico che non viene escluso dalle *Audit Whitelist* passa a questo livello e tutti i *log* che fanno *match* con queste regole non produrranno *Alert* o *Incident*.

Alert Whitelist

Permette di specificare quale tipologia di minaccia escludere, indicando sorgenti e destinazioni. È possibile applicarle a gruppi specifici e riferire ai *Rule ID* delle minacce contenute nel database interno del CyberCommand. Il *form* mostrato in Figura 5.10 è molto più specifico rispetto a quello delle *Audit Whitelist*.

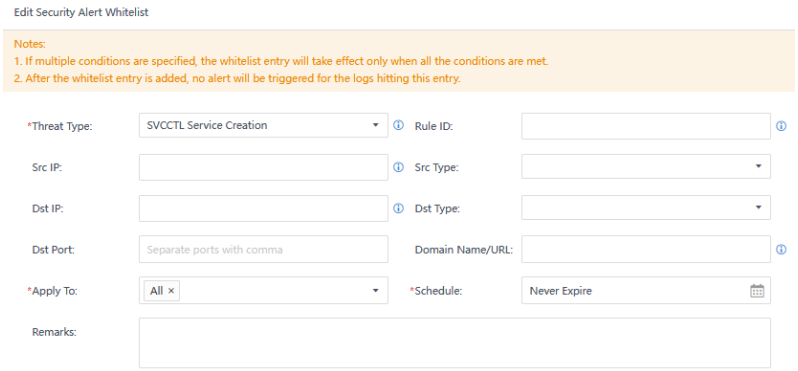


Figura 5.11: Definizione di una *Alert Whitelist*

Weakness Scan Whitelist

Permettono di specificare quali rischi escludere dalle segnalazioni, ad esempio per situazioni note o con rischio minimo tale da essere ignorato. Se fatte direttamente dalla scheda di un rischio rilevato è il CyberCommand a consigliare il *Rule ID* di riferimento, ma anche solo con IP/URL e *Risk Type* la regola funziona. La definizione di una *Weakness Scan Whitelist* è mostrata in Figura 5.12.

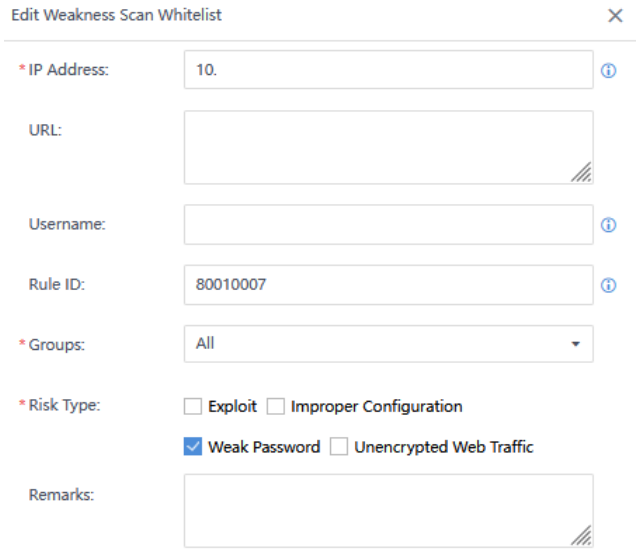


Figura 5.12: Definizione di una *Weakness Scan Whitelist*

5.4 Remediation

Il CyberCommand permette di configurare delle *remediation*, ovvero una serie azioni in risposta a determinati eventi. Queste possono integrarsi con gli altri strumenti di Sangfor, come *Endpoint Secure* (ES) e *Network Next Generation Firewall* (NGAF). Vengono create tramite uno strumento grafico che permette di definire un diagramma di flusso sfruttando degli elementi preimpostati offerti dal sistema, un esempio è mostrato in Figura 5.13. Le *remediation* possono essere configurate per avviarsi in automatico alla rilevazione di un particolare evento oppure manualmente, in modo da velocizzare la risposta agli eventi più comuni. Verranno discusse nel dettaglio nel capitolo successivo nella sezione 6.5.

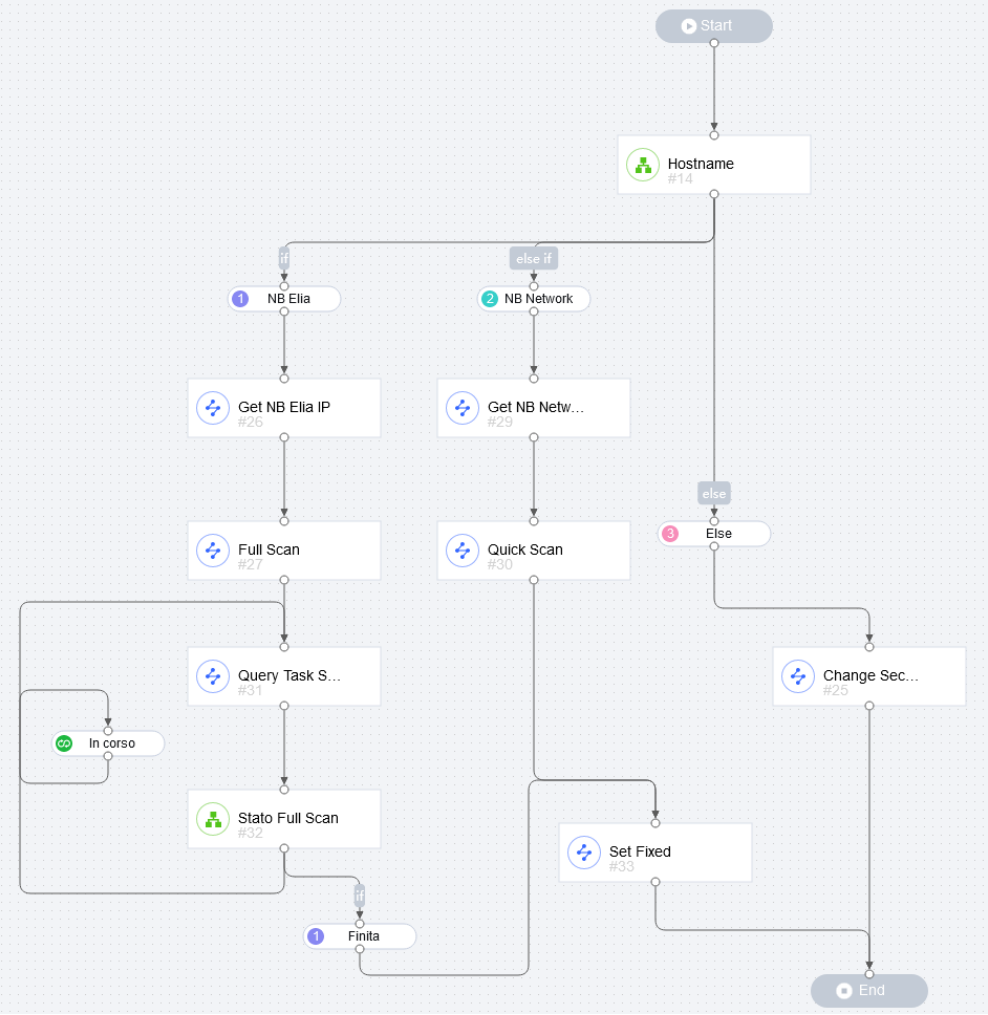


Figura 5.13: Definizione di una *remediation*

I componenti di queste regole di *remediation*, dette *Policy*, sono:

5.4.1 Action Node

Sono i nodi della *policy*, mostrati in Figura 5.14 dove vengono identificate le azioni da eseguire. Queste sono scelte tra una lista di azioni preimpostate, in base allo strumento che andrà ad eseguirla, ad esempio CyberCommand, *EDR* o altri. Il *Device IP* è sempre quello di chi agisce. Ogni azione ha la possibilità di definire un *delay* di esecuzione per permettere la temporizzazione delle azioni o attesa di altri eventi.

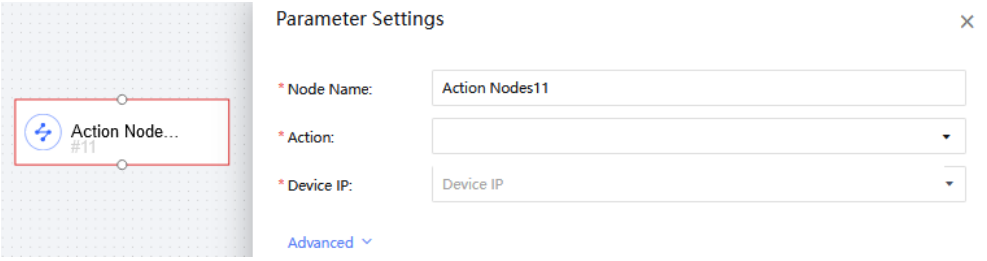


Figura 5.14: Elemento *Action Node*

5.4.2 Decision Node

Sono i nodi che permettono di prendere decisioni, mostrati in Figura 5.15. Permettono di creare una struttura di *if-then-else* in cui definire vari *branch* da seguire in base a determinate condizioni. I parametri utilizzabili sono definiti internamente dagli strumenti e vengono selezionati tramite un menù a tendina.

Per andare a simulare dei cicli viene utilizzato un sistema di *loopback* che permette di tornare ad un nodo precedente in caso di particolari risultati o condizioni, fino ad un massimo di 10 volte.

5.5 Report

Il CyberCommand permette di generare dei *report*, su richiesta o in automatico, sullo stato della rete, raccogliendo tutti le segnalazioni rilevate, dispositivi coinvolti e azioni intraprese.

Questi possono essere generati in formato *PDF* e inviati automaticamente via *email*, oppure possono essere consultati direttamente dal sistema.

Possono essere molto utili come supporto per la dimostrazione ai clienti di quanto questo sistema, che lavora silenziosamente in *background*, sia in grado di rilevare e risolvere problemi di sicurezza.

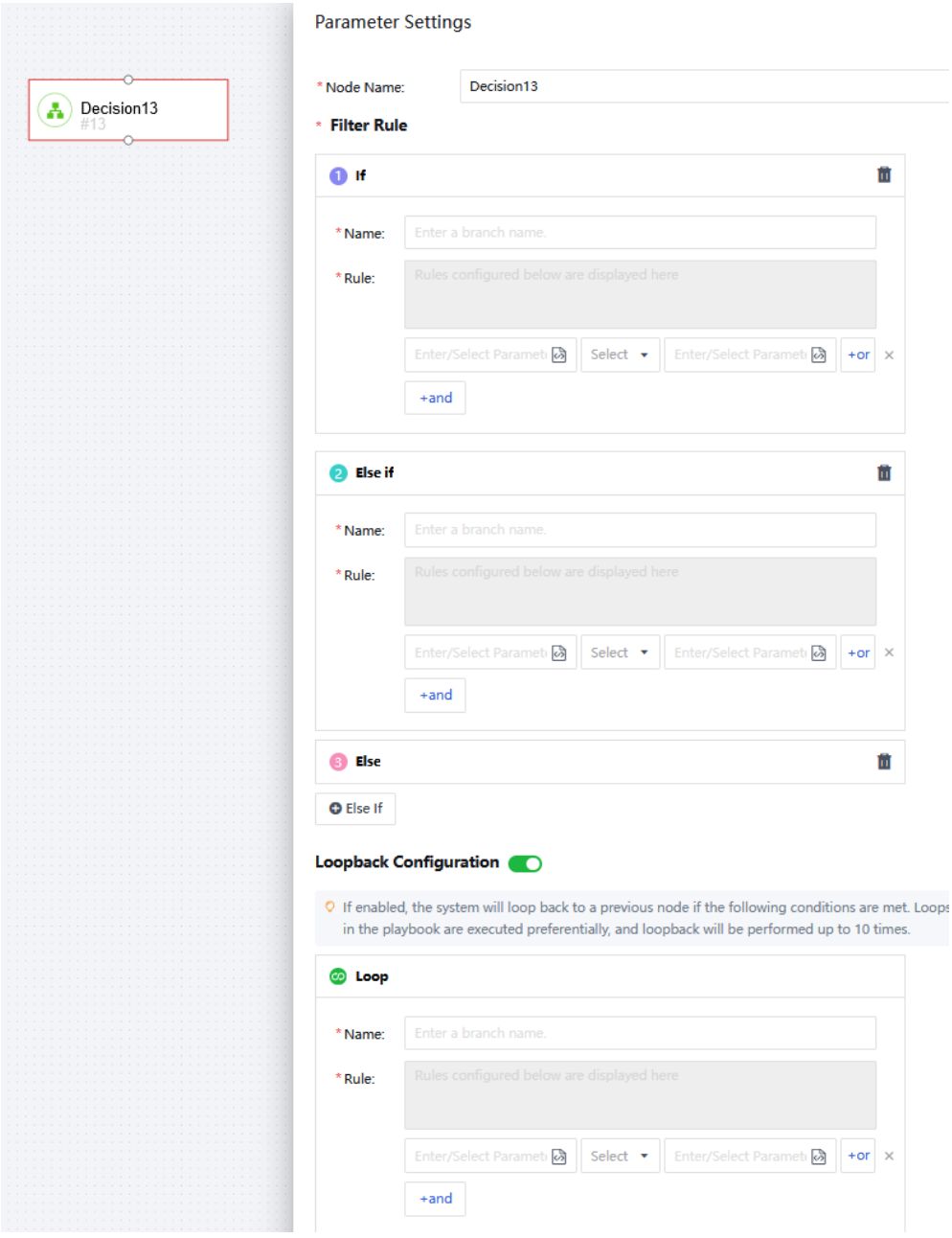


Figura 5.15: Elemento *Decision Node*

Capitolo 6

Svolgimento dello stage

Qui vengono raccolte tutte le principali attività svolte e osservazioni sul prodotto.

6.1 Analisi dei requisiti minimi del sistema

Nei primi giorni in azienda era stato organizzato un'incontro formativo sul sistema di NDR da parte del fornitore, a cui mi è stato permesso di partecipare per seguire la presentazione di Sangfor. In questo incontro sono stati mostrati i vari strumenti che compongono il sistema di NDR e sono stati spiegati i concetti di base e casi d'uso. Vengono venduti in versione fisica *on-premise* o virtualizzata, su cui è ricaduta la scelta di Wintech.

Dalle schede tecniche dei prodotti è possibile vedere le specifiche delle macchine e i requisiti minimi richiesti per la virtualizzazione. Questi sono stati raccolti rispettivamente in Tabella 6.1 e Tabella 6.2.

CyberCommand	**Sonda STA**
Memoria fino a 256GB di RAM	Fino a 32GB di RAM
Fino a 20 core di CPU	Fino a 8 porte 10/100/1000 BaseT
Supporto al RAID50	Fino a 8 porte GBe SFP e fino a 4 porte 10GBe SFP+
Dimensioni fisiche: 2U	In versioni da 1U e 2U
	Supporta fino a 12 interfacce di rete

Tabella 6.1: Scheda tecnica degli apparati fisici

CyberCommand	**Sonda STA**
ISO basata su CentOS 7	ISO basata su CentOS 7
Capacità di gestione fino a 7Gbps di traffico	Capacità di gestione fino a 2Gbps di traffico
Supporta solo HCI o piattaforme certificate VMWare	Supporta solo piattaforme VMWare

Tabella 6.2: Requisiti minimi per le macchine virtuali

6.2 Progettazione

Al momento del mio arrivo in Wintech il sistema era stato appena installato e con una prima configurazione di base con una singola sonda, come *Proof of Concept*. I primi giorni sono stati dedicati alla definizione delle configurazioni di un secondo NUC e del sistema di NDR, che è stato poi utilizzato per monitorare la rete interna dell'azienda.

Tutti i vari schemi di rete sono raccolti in Appendice A. Lo scopo di questi non è di essere una rappresentazione estremamente tecnica e dettagliata, ma più quello di dare un'idea generale e supporto grafico a quanto viene descritto testualmente.

6.2.1 Posizionamento delle sonde

Durante il corso di presentazione del fornitore è stata presentata una possibile configurazione (sezione A.1) di base per dove posizionare le sonde STA [11].

Come consigliato dal produttore, posizionarle tra i vari dispositivi permette loro di andare a monitorare anche traffico interno, riuscendo ad individuare i cosiddetti *movimenti laterali* e possibili attacchi che non passano dall'esterno, come ad esempio l'espansione del controllo da parte di un *malware* sui dispositivi.

In Wintech le varie sonde sono state dislocate una in sede, due tra i *data center* e una da un cliente (schema in sezione A.2)

6.2.2 Configurazione dei dispositivi

Come descritto nella sezione 6.1 i dispositivi sono stati virtualizzati tramite l'*hypervisor ESXi* di *VMWare*. Questo prodotto era già conosciuto e in uso in Wintech, è stato solamente necessario adattare la configurazione per permettere alle sonde virtuali di funzionare correttamente avendo le interfacce di rete configurate per effettuare il *mirroring* del traffico. Per fare questo sono stati utilizzati i *commutatori virtuali* e i *gruppi di porte*. Inoltre, per rendere i dispositivi tolleranti a perdita di corrente è stato configurato l'avvio automatico del sistema e delle macchine virtuali.

Un problema riscontrato con il *software* di virtualizzazione è stata l'incompatibilità con gli *E-Core* dei nuovi processori *Intel* presenti nei NUC. Al momento l'unica soluzione è stata quella di disabilitarli, andando a sfruttare solo gli altri *P-Core*, che sono comunque sufficienti per le esigenze del sistema.

6.3 Controllo delle segnalazioni

Uno dei punti chiave di uno strumento di questo tipo è quello di fornire segnalazioni utili all'amministratore per monitorare lo stato della rete. Durante tutto il periodo di stage il primo obiettivo è stato quello di capire quali fossero quelle più utili e come poterle sfruttare al meglio.

Ogni giorno una delle prime attività era proprio il controllo delle ultime segnalazioni, per capire se durante la notte ci fossero stati strani comportamenti nella rete. Dopo le prime settimane, dove sono state definite una serie di *whitelist* per evitare falsi positivi, si è arrivati ad un sistema che segnalava solo i problemi più importanti e che richiedevano un controllo manuale da parte di un amministratore.

Principalmente sono stati esclusi tutti i problemi legati a sistemi in fase di test del *team* di ricerca e sviluppo, le comunicazioni tra i *software* di monitoraggio come PRTG e altri di *backup*. Molto spesso *scan* di rete effettuati in modalità automatica

e generica da attaccanti che cercavano di trovare dispositivi vulnerabili portavano a segnalazioni di porte aperte note, ad esempio la 80 e la 443 per il sito *web* aziendale.

6.3.1 Segnalazioni di server security

In generale le segnalazioni di *Server Security* (sottosezione 5.1.2) permettono di trovare anche problemi dovuti a configurazioni errate o a problemi di sicurezza non ancora risolti. In particolare, durante lo stage, sono state utili:

- la funzione di rilevazione delle *password* deboli, che è stata utilizzata definendo all'interno della lista di *password* da segnalare alcune utilizzate in passato e che devono essere dismesse per motivi di sicurezza. In questo modo è stato possibile rilevare alcuni utenti che le utilizzavano ancora e che sono stati avvisati di cambiarle.
- tramite le segnalazioni *Unencrypted Web Traffic* invece è stato possibile rilevare alcuni servizi di clienti in *full-outsourcing* che non utilizzavano la versione sicura di HTTP. Questo ha permesso di avvisarli e di proporre loro una soluzione per risolvere il problema.
- la categoria *Improper Configuration* che ha permesso di verificare se alcune configurazioni contengono errori noti o piccole dimenticanze che possono portare a problemi di sicurezza. Può tornare utile per rilevare situazioni in cui erano state aperte porte non standard per permettere l'accesso a servizi interni che non erano poi state chiuse dopo aver terminato il lavoro.

6.3.2 Esempio di segnalazione: Infezione da *Cryptominer*

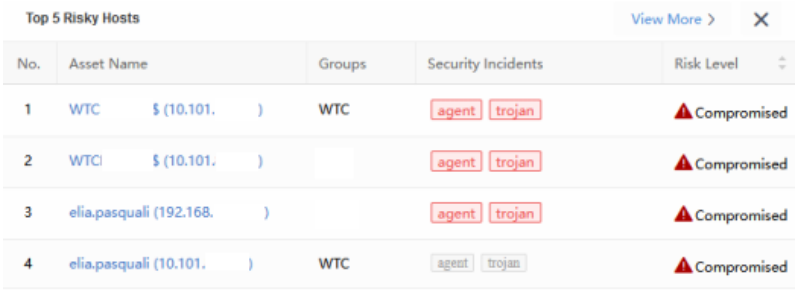


Figura 6.1: Segnalazioni di *Cryptomining* in *Host Security*

Nella Figura 6.1 possiamo vedere la situazione rilevata dal sistema NDR dopo che ho effettuato delle connessioni a siti legati a *pool* di *cryptomining*. Questo è stato fatto per testare il sistema e capire come funzionasse.

Dopo aver rilevato il traffico, ha segnalato l'host che ha effettuato le connessioni come compromesso, in quanto potenzialmente infetto da un *miner* di criptovalute. Un difetto riscontrato nella segnalazione è che il mio dispositivo veniva rilevato più volte, in base a come questo si presentava sulla rete.

Discutendone con il tutor siamo arrivati alla conclusione che questo è legato alla struttura interna della rete Wintech e a come Windows gestisce le sue interfacce di rete e i nomi utente, che insieme al posizionamento consigliato per le sonde lo rende un problema di difficile risoluzione.

6.3.3 Esempio di segnalazione: Richieste DNS malevole

Un esempio che mostra come il sistema NDR analizza il traffico sono le segnalazioni legate a traffici DNS considerati malevoli. Durante il periodo di stage questa tipologia è stata oggetto di studio per capire come configurare al meglio il posizionamento del sistema e come definire una serie di *whitelist* per evitare falsi positivi senza lasciare troppo traffico non controllato.

Le sonde, per loro natura e posizionamento interno alla rete, analizzano il traffico che passa "attraverso i cavi", rilevando quindi anche possibili attacchi che si proliferano tramite *movimento laterale*. Questo porta ad avere segnalazioni di compromissione per ogni dispositivo in cui la richiesta DNS che il sistema ha catalogato come malevola transita.

Un piccolo diagramma qualitativo di questo processo è mostrato in sezione A.3, dove un dispositivo a dominio effettua una richiesta considerata malevola che passa per *Domain Controller* e successivamente il *firewall*.

6.4 Test del prodotto

Durante tutto il periodo di stage il sistema era attivo sulla rete e questo mi ha permesso di andare a testarlo in tutte le sue funzionalità e trovare i suoi limiti.

6.4.1 Rilevazione di attacchi

Tutti gli eventi malevoli scatenati per testare i tempi di risposta del sistema hanno mostrato che le rilevazioni sono quasi immediate, con ritardi dovuti solo al tempo di propagazione del traffico sulla rete. Una volta, dopo un'intensiva sessione di test che ha generato un'elevata dose di traffico, il sistema ha smesso di funzionare correttamente.

Questo problema è stato difficile da comprendere dato che la *webapp* continuava ad essere attiva, semplicemente non era possibile interagire con i *log*. Per prima cosa si è partiti con un'analisi diagnostica dello stato di salute del sistema, dal NUC alla macchina virtuale, che però non mostrava nessun problema. Dopo aver contattato il supporto, abbiamo scoperto che tutto ciò era dovuto ad un errore di configurazione della politica di rotazione dei *log* e alla soglia critica impostata, che ha portato ad un blocco del disco virtuale.

La configurazione da correggere, essendo un parametro all'interno del *database* del sistema, basato su *ElasticSearch*, non era accessibile dall'interfaccia web, ma solo tramite *SSH* e con credenziali non disponibili a noi. Dopo che il supporto ha corretto il problema, abbiamo provveduto ad aumentare lo spazio a disposizione della macchina, che era stato volutamente assegnato in quantità limitata per verificare se il requisito richiesto fosse effettivamente necessario e non fosse stato sovrastimato. Questa modifica ha rimesso in funzione il sistema e impedito al problema di ripresentarsi.

6.4.2 Rilevazione di falle di sicurezza

Come descritto nella sottosezione 5.1.2 il sistema è stato in grado di rilevare anche falle di sicurezza e configurazioni errate. Questo ha permesso di attivare i vari *team* per occuparsi di questi problemi, passando da una prima analisi alla ricerca di soluzioni non invasive per il cliente, fino all'avviso di questi ultimi e alla proposta di soluzioni per risolvere i problemi.

6.4.3 Rilevazione di *malware*

Spesso il sistema NDR si è rivelato attento ad ogni possibile strumento che operava in maniera malevola all'interno della rete. Sono stati utilizzati alcuni strumenti di *crack* per le licenze di prodotti a pagamento per verificare la capacità di rilevazione di questo tipo di software. Bisogna considerare però che essendo un prodotto per la sicurezza della rete, non è in grado di rilevare software malevolo che lavora solamente in locale, ma solo se questo effettua connessioni verso l'esterno, per operazioni di *command and control*, come nel caso esempio del *cryptominer* (sottosezione 6.3.2).

6.4.4 Usabilità

Uno dei primi problemi riscontrati è stato quello di capire come utilizzare il sistema e come interpretare le segnalazioni. Per quanto l'interfaccia sia abbastanza intuitiva e rivolta ad un utenza con un minimo di bagaglio tecnico per comprendere ciò che viene mostrato, è comunque necessario un periodo di apprendimento per capire come utilizzare al meglio il sistema. Un fattore che ha rallentato alcune operazioni di configurazione è stata la documentazione non aggiornata o non completa. Questo ha portato a dover capire cosa alcune funzioni facessero tramite prove ed errori.

Molte volte le configurazioni potevano essere trovate sparse tra vari menù, inoltre spesso alcuni *link* portavano senza preavviso ad altre pagine, che non essendo ben segnalate, erano difficili da raggiungere nuovamente successivamente. Molto spesso i parametri non avevano nomi parlanti, rendendo difficile comprendere il loro utilizzo. Questa situazione potrebbe essere dovuta allo sviluppo in Asia poi adattato per altri mercati, portando a delle traduzioni non sempre precise.

Nonostante tutto, questo problema è stato parzialmente limitato dall'estrema disponibilità del fornitore, che ha sempre cercato di risolvere i problemi e di fornire spiegazioni e chiarimenti, tramite scambi di email e sessioni di discussione e supporto remoto.

6.5 Remediation

Una delle funzionalità più interessanti del sistema NDR è proprio quella di andare a risolvere autonomamente, dopo previa configurazione, alcuni problemi di sicurezza. Questo permette di avere un sistema che non solo rileva e segnala i problemi, ma che cerca anche di risolverli, permettendo di avere un sistema di sicurezza più completo e che richiede meno interventi manuali, evitando rallentamenti dovuti a tempi di risposta o assenza di operatori qualificati.

Come per le altre funzionalità, anche questa mancava di una documentazione adeguata, rendendo quindi necessaria una fase di studio e di test per capire come funzionasse e come poterla configurare al meglio. Dopo primi test basilari che andavano a lavorare internamente alla *webapp* sul singolo dispositivo CyberCommand[12] sono passato a testare l'integrazione con il sistema di *Endpoint Protection* di *Sangfor*[13].

6.5.1 Esempio di remediation: scansione antivirus automatica

Partiamo dalla definizione della policy, mostrata in Figura 6.2

Vediamo che è stata definita in modo da attivarsi quando viene rilevato un *Incident* della categoria *Trojan* e solo se il dispositivo interessato è un *Host*, questo per escludere

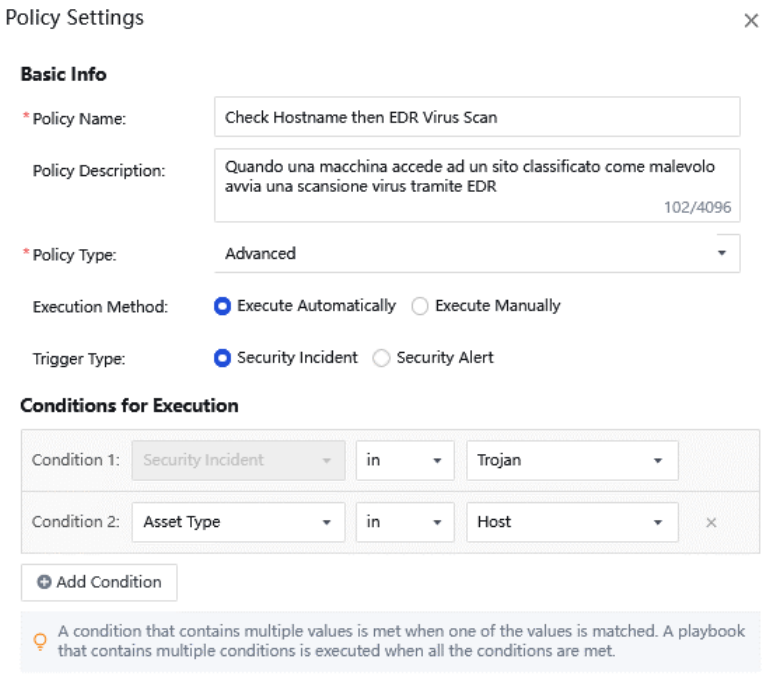


Figura 6.2: Policy per la scansione antivirus automatica

altri dispositivi di rete in cui richieste malevole transitano e non è possibile effettuare una scansione antivirus. La *policy* è stata impostata per avviarsi in automatico.

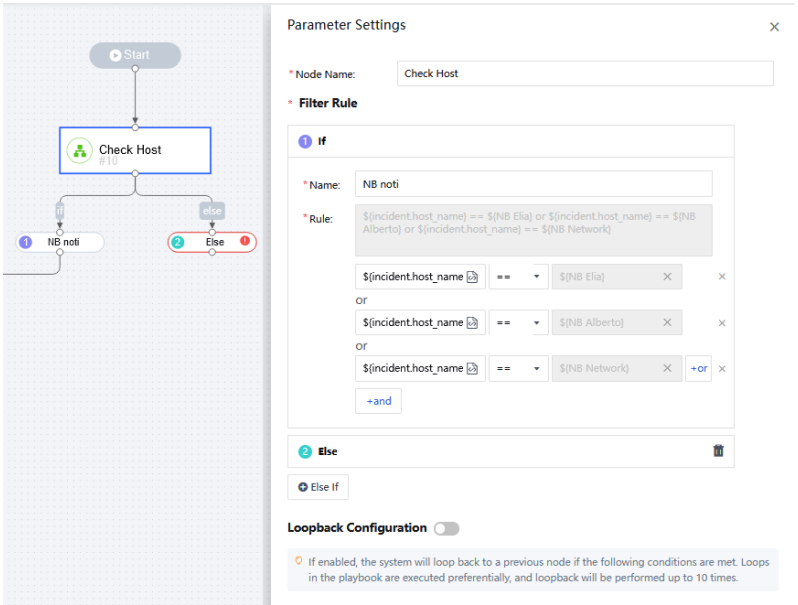


Figura 6.3: *Decision node* per filtrare i dispositivi

In Figura 6.3 ho inserito un primo filtro per lavorare solamente su notebook che

potevo "disturbare" durante i miei test, come il mio o quelli di altri stagisti. Questo è stato ottenuto tramite un *decision node* che filtra i dispositivi in base al nome utente, che è stato impostato in fase di configurazione del sistema, salvati in una serie di costanti. Questo filtro è stato necessario per evitare di andare a disturbare i clienti con richieste di scansione antivirus.

Tutta la parte di effettiva attivazione della scansione si può vedere in Figura 6.4. Tramite un *action node* si avvia sul programma *EDR* installato sul dispositivo una scansione di tipo *Full Scan* (Figura 6.5). Successivamente si è aggiunto un *decision node* che controlla se la scansione è terminata con successo o meno, sfruttando il sistema di *loopback* per ricontrollarne lo stato fino alla terminazione, con successo o meno.

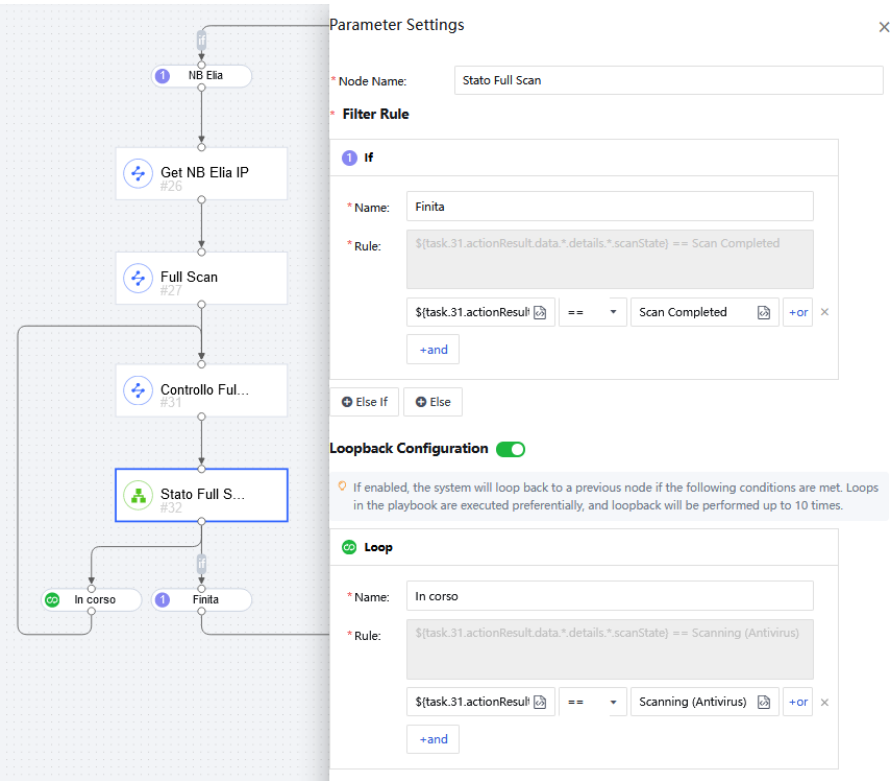


Figura 6.4: Configurazione della scansione

6.5.2 Problemi riscontrati

Durante la configurazione di questa funzionalità sono stati riscontrati diversi problemi, alcuni dei quali sono stati risolti tramite l'assistenza del fornitore, altri invece sono ancora presenti.

Problemi nella gestione dei parametri multipli

Il sistema permette di definire regole con parametri multipli, divisi da virgole. In caso di parametri predefiniti o costanti, che vengono salvati come stringhe e poi recuperati tramite la sintassi `$nome_parametro`, viene mostrato un errore e limitato ad un singolo simbolo `$`, come mostrato in Figura 6.6

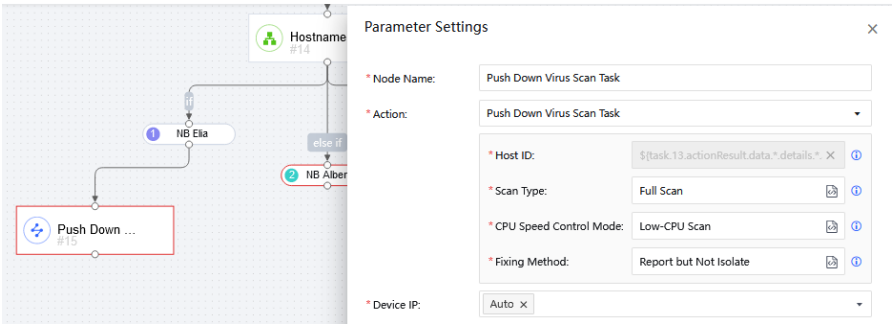


Figura 6.5: *Action node* per avviare la scansione

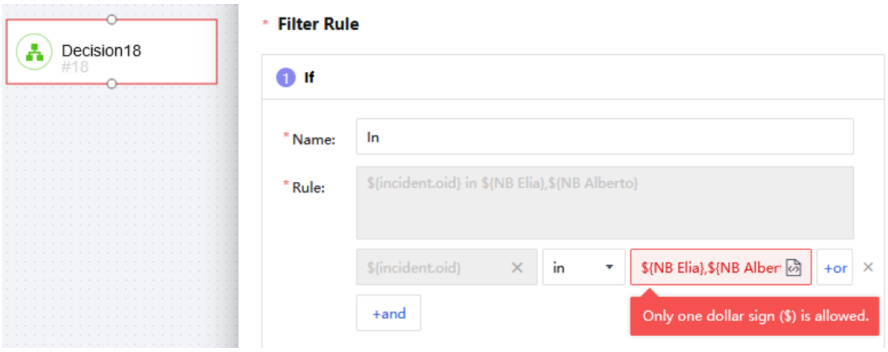


Figura 6.6: Errore nella gestione dei parametri multipli

Mancanza di documentazione

Per prima cosa, come già accennato, la documentazione non era completa e non era possibile capire come funzionasse la funzionalità senza fare dei test. Dopo aver fatto delle ricerche sul forum della community[14] di *Sangfor* ho trovato un post che accennava a dei documenti, che però non erano disponibili. Dopo aver contattato il *team* italiano, mi è stato fornito un documento con la raccolta dei parametri disponibili per la configurazione delle *policy*, anche se non era ancora completo[15].

Mancanza di feedback sullo stato della scansione

Per ottenere un feedback sullo stato delle azioni era necessario andare a controllare i *log* in una sezione non facilmente raggiungibile. Questi però si limitavano a mostrare se l'azione aveva completato con successo o meno, con piccole informazioni sugli errori, come mostrato in Figura 6.7. Questo ha portato a dover fare diversi test per capire come funzionasse la funzionalità e come poterla configurare al meglio.

Mancanza di un sistema di test

Un altro problema riscontrato è stato quello di non avere un sistema di test per verificare il funzionamento delle *policy* prima di applicarle. Questo ha portato a dover fare diversi test scatenando falsi positivi, rallentando la configurazione delle risposte.

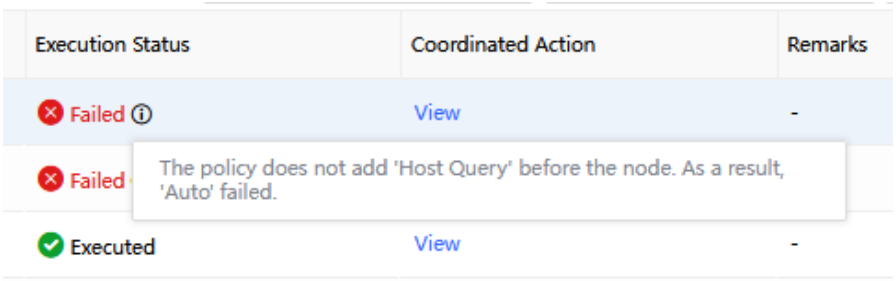


Figura 6.7: Esempio di *log* di errore

Limitazioni nelle integrazioni

Questo problema è legato al fatto che il prodotto è ancora nuovo. Per offrire l'integrazione con strumenti di terze parti è necessario per il *team* di sviluppo di *Sangfor* ottenere un'interfaccia di programmazione (*API*) da parte dei competitor. Dopo un dialogo con il *team* italiano ci è stato detto che tutto questo è attualmente una delle priorità del produttore.

Definizione delle policy macchinosa

La definizione di *policy* tramite questo strumento grafico riesce ad essere intuitivo e va a limitare la mancanza di documentazione su come produrre queste regole. Forse a causa della mia formazione informatica, ho trovato che la definizione di queste regole fosse macchinosa e sarebbe stata estremamente più chiara e manutenibile se fosse stata definibile tramite uno strumento testuale, come ad esempio un linguaggio di *scripting*.

Tramite regole testuali sarebbe stato possibile anche definire delle *policy* tramite un sistema di *template*, che avrebbe permesso di velocizzare la configurazione e di avere un sistema di test più semplice. Inoltre, si sarebbe potuto sfruttare un sistema di versionamento come *Git*, per tenere traccia delle modifiche apportate e per poter effettuare *rollback* in caso di problemi.

6.6 Report tramite API REST

Le funzionalità di creazione di *report* offerte dal sistema si limitavano alla produzione di *file* PDF con un consuntivo sull'andamento e lo stato della rete rispetto ad un particolare periodo. Utilizzando lo strumento però si sentiva la necessità di estrarre dei dati in formati strutturati come *JSON* o *CSV* per poterli utilizzare in altri strumenti, ad esempio integrandoli agli altri sistemi di monitoraggio o creando delle *dashboard* personalizzate con lo stack ELK, ovvero *Logstash* per processare i dati, *ElasticSearch* per l'indicizzazione e *Kibana* per la visualizzazione.

6.6.1 Problemi riscontrati

Il primo problema riscontrato è stato quello di capire come funzionasse il sistema di autenticazione per le API. Dopo aver fatto delle ricerche sul forum della community[14] di *Sangfor* ho trovato un *post* che conteneva al suo interno un documento[16], che sembrava essere abbastanza recente.

Dopo alcune prove, che non hanno portato ad alcun risultato, ho contattato il *team* di supporto, che mi ha confermato che il documento si riferiva ad una versione precedente del sistema, che non era più valido e che non era disponibile una documentazione aggiornata, dato che era in programma un aggiornamento importante del sistema con una probabile riscrittura di queste funzionalità.

6.6.2 Soluzione alternativa

Per ottenere dei dati dall'NDR in un formato utile al mio scopo ho cercato di estrarli dalle richieste che vengono effettuate normalmente dalla *webapp*, analizzandole tramite gli strumenti da sviluppatore integrati nei *browser*. Questa via non ha portato a risultati soddisfacenti, quindi sono passato ad una tecnica più invasiva, tramite del *web scraping* con *Python*, sfruttando la libreria *Selenium* e *requests* per estrarre i dati dalle pagine.

Nonostante questo, la soluzione è risultata essere molto macchinosa e poco performante, in quanto richiedeva di simulare l'accesso alla *webapp* e di navigare tra le varie pagine per estrarre i dati. Inoltre, il sistema di autenticazione tramite *token* ha portato a dover aggiornare manualmente il codice ogni volta che questo cambiava, rendendo la soluzione poco manutenibile.

Capitolo 7

Conclusioni

7.1 Obbiettivi raggiunti

Rispetto agli obiettivi descritti nella sottosezione 3.2.3:

- Per la categoria **Obbligatori** il *deploy* e la configurazione del prodotto è avvenuta. Il sistema è stato testato e le *remediation* analizzate e definite, nei limiti dell'integrazione con sistemi di terze parti. Tutte le operazioni sono state documentate e sono state scritte le procedure per la gestione del sistema.
- Per la categoria **Desiderabili** invece non è stato possibile integrare ulteriori apparati dell'infrastruttura di Wintech oltre all'*EDR* di Sangfor.
- Sempre per gli stessi motivi, anche la categoria **Facoltativi** ha risentito della mancanza di integrazioni con sistemi di terze parti. Inoltre, tutti i test effettuati sono stati rilevati, confermando la capacità del sistema di rilevare anche attacchi interni alla rete.

7.2 Segnalazioni e miglioramenti proposti

Al termine del percorso di stage ho raccolto tutte i problemi riscontrati, come ad esempio la gestione dei parametri multipli, e i miglioramenti possibili, come la definizione di *policy* tramite linguaggio di *scripting*. Tutto questo è stato discusso con il tutor e poi riportato al fornitore tramite il *team* italiano, che ha ringraziato e poi provveduto a inoltrare il resoconto dell'esperienza al *team* di sviluppo.

7.3 Valutazione personale

7.3.1 Conoscenze tecniche acquisite

La scelta di un progetto in questo ambito mi ha permesso di approfondire il campo delle reti dal lato pratico, cosa che per ovvie ragioni è difficile da vedere durante il corso di studi. Lavorare con strumentazione reale e di livello *enterprise* mi ha permesso di vedere come vengono gestiti i sistemi in un contesto aziendale, espandendo la mia visione che si limitava a simulazioni e piccoli progetti personali con *container* e *virtual machine*.

Ascoltando consigli di colleghi e tutor, ho potuto capire come spesso in un contesto del genere è necessario scegliere un *trade-off* tra la soluzione teorica più elegante e le limitazioni imposte dall'ambiente in cui un particolare sistema o strumento andrà a operare.

Aver utilizzato uno strumento di NDR mi ha permesso di capire come funzionano i sistemi di rilevazione all'avanguardia e come sia necessario un continuo aggiornamento per stare al passo con le minacce sempre più sofisticate.

7.3.2 Conoscenze personali acquisite

Un percorso di questo tipo mi ha permesso di inserirmi per un periodo di tempo abbastanza importante nel mondo del lavoro. Questo mi ha fatto capire come funziona un'azienda, come si lavora in un *team* e come si gestiscono le scadenze e le priorità.

A differenza dei progetti durante il corso di studi, tra amici, con scadenze molto più flessibili e con un margine di errore più ampio, in un contesto aziendale è necessario rispettare le richieste e le tempistiche, per non compromettere il lavoro di altri colleghi.

Inoltre, ho avuto occasione di interagire con clienti e fornitori e questo mi ha permesso di capire come gestire le relazioni con le persone in contesti lavorativi, in modo da poter ottenere il massimo risultato da ogni interazione.

7.3.3 Gap tra Università e mondo del lavoro

In un corso di studi come quello di Informatica è impossibile coprire tutti gli argomenti e le tecnologie che nascono e si evolvono ogni giorno. Tuttavia la base fornita è estremamente solida e permette di affrontare un problema o lo studio di nuove tecnologie in modo autonomo.

Nel mio caso particolare, come detto prima, ho potuto toccare con mano un campo che non viene trattato durante il corso di studi nella pratica, ma solo nella teoria. Dal lato della gestione del progetto invece forse solo il progetto di Ingegneria del Software riesce a dare un'idea di scadenze e tempistiche da rispettare.

Appendice A

Schemi di rete

A.1 Slide Sangfor: posizionamento consigliato delle sonde

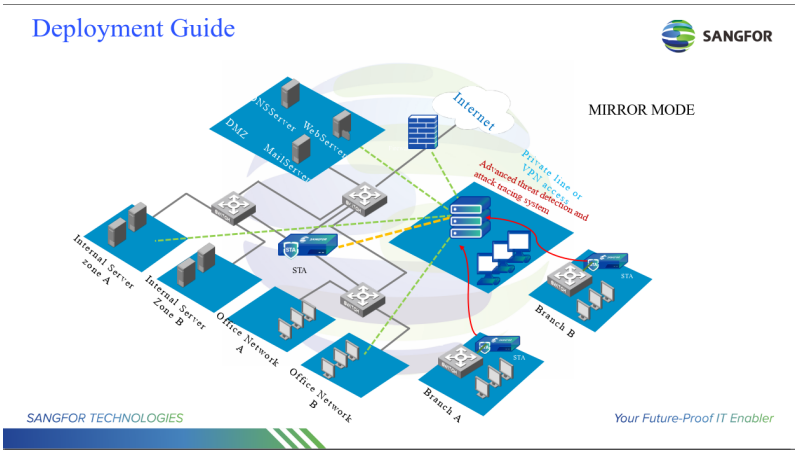


Figura A.1: Configurazione di esempio del produttore

A.2 Rete Wintech: posizionamento delle sonde tra le sedi

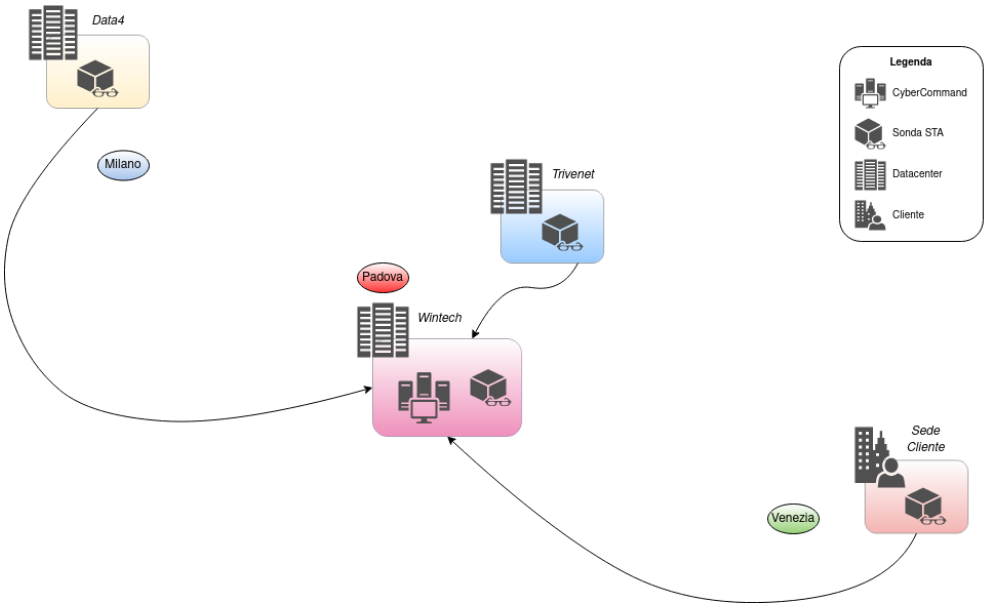


Figura A.2: Posizionamento delle sonde

A.3 Segnalazione richieste DNS malevole: schema qualitativo

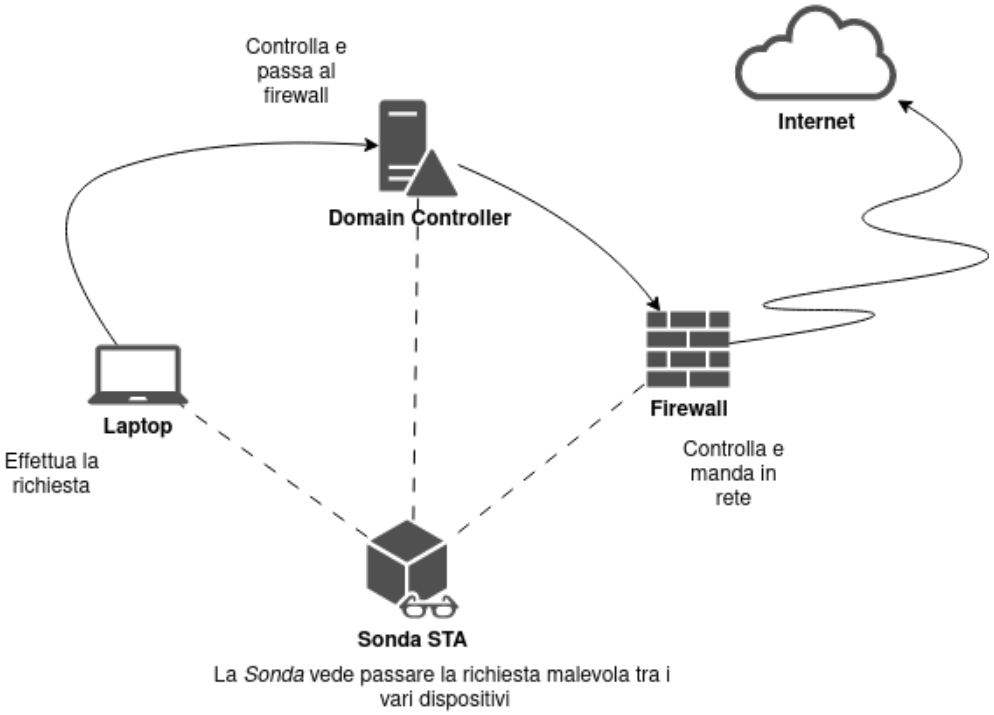


Figura A.3: Richieste DNS rilevate dal sistema

Appendice B

Attacchi e mitigazioni

B.1 Slowloris DDoS Attack

Un attacco che è possibile attuare sfruttando delle richieste HTTP è detto *Slowloris DDos Attack*[17]. Questo agisce riempiendo la vittima di richieste di apertura di connessioni HTTP, che vengono mantenute aperte per il tempo massimo possibile per poi mandare una particolare richiesta per mantenerla attiva facendo credere di avere semplicemente una connessione lenta. Utilizzando più richieste in contemporanea è possibile saturare la vittima, che non sarà più in grado di accettare ed aprire nuove connessioni, risultando in un *Denial of Service*. Questo attacco è particolarmente efficace perché non richiede molte risorse.

B.2 DNS Amplification Attack

Gli attacchi di tipo *DNS amplification*[18] sfruttano il fatto che il protocollo DNS utilizza UDP per le sue comunicazioni. Creando richieste con DNS che contengono come mittente l'indirizzo IP della vittima che vogliamo attaccare, il server DNS gli risponderà senza effettuare controlli. Se le richieste sono effettuate in massa da più macchine è possibile andare a saturare la banda della vittima, incrementando di svariate volte il volume di traffico generato dall'attaccante a discapito di un maggiore utilizzo di un server DNS pubblico, utilizzato inutilmente, ottenendo un attacco di tipo *Denial of Service* distribuito (*DDoS*).

B.3 DNS Sinkhole - Mitigation Strategy

Una tecnica di difesa invece da richieste DNS malevole è quella di utilizzare un *DNS Sinkhole*[19]. Questa tecnica consiste nel configurare il firewall in modo da rispondere a particolari richieste che consideriamo malevole con con un indirizzo IP fittizio. Questo porterà l'attaccante a contattare direttamente questo falso IP, senza però riuscire a collegarsi davvero, rallentandolo e permettendolo di identificarlo anche se sta usando un *server* DNS interno. Questa tecnica è molto efficace perché non richiede molte risorse e può essere facilmente implementata.

B.4 Domain Generation Algorithm

Un *Domain Generation Algorithm* (DGA) è un algoritmo utilizzato per generare domini che possono essere utilizzati per comunicare con i server di controllo. Questo permette di rendere più difficile la rilevazione e la chiusura dei server di controllo, in quanto non è possibile bloccare un singolo dominio, ma bisogna bloccare tutti quelli generati dall'algoritmo. Questo tipo di algoritmo è stato alla base delle comunicazioni ai propri server di *Command and Control* (C&C) nei malware *Conficker*[20] nel 2008 o *QSnatch*[21] nel 2020.

Un metodo per utilizzare un DGA è quello di generare un dominio a partire da una data come *seed*, in modo che l'attaccante possa prevedere il dominio che verrà generato in futuro, in modo da poterlo registrare in anticipo, dato spesso domini appena registrati vengono considerati inaffidabili e quindi bloccati.

Bibliografia

Riferimenti bibliografici

[11] Sangfor, *Slide della presentazione del prodotto*. 2023 (cit. a p. 35).

[12] Sangfor, *Sangfor CyberCommand Playbook Policy Training*. apr. 2023 (cit. a p. 38).

[13] Sangfor, *Best Practices for Configuration - How to Correlate with Endpoint Sec*. apr. 2023 (cit. a p. 38).

[15] Sangfor, *Parameter specification of CyberCommand response actions*. mar. 2023 (cit. a p. 41).

[16] Sangfor, *Sangfor Cyber Command Restful API to 3rd Party*. apr. 2023 (cit. a p. 42).

Siti web consultati

[1] «I nostri plus - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/siamo/i-nostri-plus/ (cit. alle pp. 1, 5).

[2] «Cloud - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/cloud/ (cit. a p. 3).

[3] «Security - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/innoviamo/che-innovazione-cerchi/security/ (cit. a p. 4).

[4] «E-Learning & Video Communication - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/innoviamo/che-innovazione-cerchi/e-learning-video-communication/ (cit. a p. 6).

[5] «ERP e Applicazioni Gestionali.» (set. 2023), indirizzo: https://www.wintech.it/innoviamo/che-innovazione-cerchi/erp-e-applicazioni-gestionali/ (cit. a p. 6).

[6] «Digital Transformation - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/innoviamo/che-innovazione-cerchi/digital-transformation/ (cit. a p. 6).

[7] «Social Collaboration & Mobility - Wintech SPA.» (set. 2023), indirizzo: https://www.wintech.it/innoviamo/che-innovazione-cerchi/social-collaboration-mobility/ (cit. a p. 6).

[8] «The Road to QUIC.» (lug. 2023), indirizzo: https://blog.cloudflare.com/the-road-to-quic/ (cit. a p. 18).

[9] «MITRE ATT&CK.» (set. 2023), indirizzo: https://attack.mitre.org/ (cit. a p. 25).

[10] «Neural-X Threat Intelligence Platform | Sangfor.» (set. 2023), indirizzo: https://www.sangfor.com/cybersecurity/innovations/neural-x (cit. a p. 26).

[14] «Sangfor Community.» (lug. 2023), indirizzo: https://community.sangfor.com/plugin.php?id=index:index (cit. alle pp. 41, 42).

[17] «Slowloris HTTP DoS | Cloudflare.» (lug. 2023), indirizzo: https://www.cloudflare.com/learning/ddos/slowloris-ddos-attack/ (cit. a p. 49).

[18] «DNS amplification DDoS Attack | Cloudflare.» (lug. 2023), indirizzo: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (cit. a p. 49).

[19] «DNS Sinkholing.» (lug. 2023), indirizzo: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/dns-sinkholing (cit. a p. 49).

[20] «Threat Brief: Understanding Domain Generation Algorithms (DGA).» (lug. 2023), indirizzo: https://unit42.paloaltonetworks.com/threat-brief-understanding-domain-generation-algorithms-dga/ (cit. a p. 50).

[21] «QSnatch Data-Stealing Malware Infected Over 62,000 QNAP NAS Devices.» (set. 2023), indirizzo: https://thehackernews.com/2020/07/qnap-nas-malware-attack.html (cit. a p. 50).

[22] «Wintech.» (set. 2023), indirizzo: https://www.wintech.it/.

[23] «Cyber Command | NDR | Cyber Threat Hunting.» (set. 2023), indirizzo: https://www.sangfor.com/cybersecurity/products/cyber-command-ndr-network-detection-and-response.